AirStation™Pro

WAPM-APG300N/WAPM-AG300N
設定事例集

このたびは、弊社製AirStationProをお買い求めいただき、誠にありがとうございます。本書は、AirStationProの各種設定事例について説明しています。ユーザーズマニュアルとあわせて本書をお読みください。

本書の使い方

本書を正しくお使いいただくための表記上の約束ごとを説明します。

■文中マーク／用語表記

⚠注意 マーク	製品の取り扱いにあたって注意すべき事項です。この注意事項に従わなかった場合、身体や製品に損傷を与えるおそれがあります。
メモ マーク	製品の取り扱いに関する補足事項、知っておくべき事項です。
▶参照 マーク	関連のある項目のページを記しています。

・文中[ ]で囲んだ名称は、操作の際に選択するメニュー、ボタン、テキストボックス、チェックボックスなどの名称を表わしています。

・文中「 」で囲んだ名称は、ソフトウェアやダイアログボックスの名称を表わしています。

・本書では原則として弊社製無線アダプタを装着したパソコンを無線パソコン、本製品の設定に使用するパソコンを設定用パソコンと表記しています。

・ケーブルで接続された10/100/1000BASEのLANとケーブルを使用しない無線LANを明確にするために本書では次の用語を使用しています。

有線LAN…ケーブルで接続されたLAN

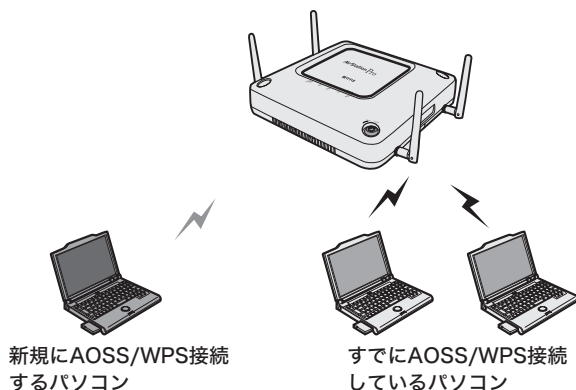
無線LAN…無線通信を使用したLAN

上記は、説明のために本書のみで便宜上使用する用語であり、一般的には使用されません。あらかじめご了承ください。

目次

例1：AOSS/WPSを使って本製品と無線接続する

本製品はAOSS/WPS機能を搭載しており、これらの規格に対応した無線機器をかんたんに接続することができます。ここではAOSSもしくはWPS（PBC）を使って、新たに無線機器を本製品に接続するための手順を紹介します。

構成例

条件

・本製品にすでにAOSS/WPS接続している無線機器がある環境に、新たな無線機器をAOSS/WPSを使って接続する。
・新たに無線機器を追加しても、既存の無線機器は接続と暗号化を維持できる。

使用機器

対象機器

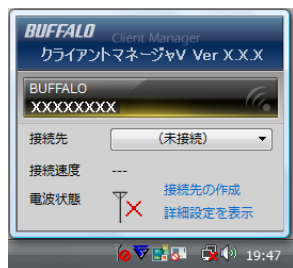
本製品（WAPM-APG300N/WAPM-AG300N）

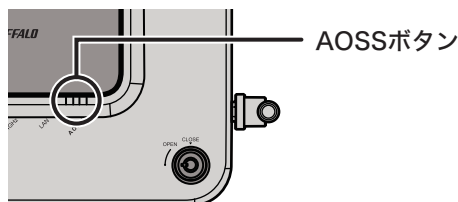
必要機器

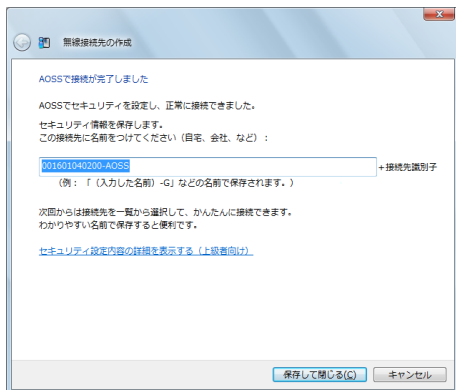
・AOSS/WPSに対応したクライアントパソコン

メモ クライアントパソコンには、あらかじめ「クライアントマネージャV」（Windows 7/Vistaの場合）または「クライアントマネージャ３」（Windows XP/2000/Me/98SE）がインストールされている必要があります。

設定手順(Windows 7/Vista)

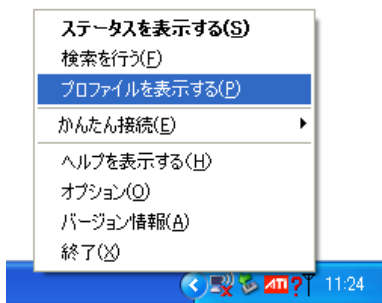
1 [スタート]－[すべてのプログラム]－[BUFFALO]－[エアステーションユーティリティ]－[クライアントマネージャV]をクリックし、「接続先の作成」をクリックします。

2 「自動セキュリティ設定」 をクリックします。

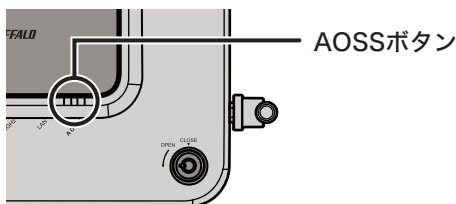
3 画面にしたがって、本製品正面にあるAOSSボタンを5GHz/2.4GHzランプが点滅するまで(約3秒間)押し続けます。

メモ 本製品正面のAOSSボタンの代わりに、本製品の設定画面([詳細設定]－[無線設定]－[AOSS])にあるAOSSボタンを押して接続設定をすることもできます。

4 接続に成功すると、30秒～1分程度してから、「接続が完了しました」と表示されます。
[保存して閉じる]をクリックします。

以上で接続は完了です。
接続完了後、「ネットワークの場所の設定」画面が表示された場合は、ご利用の環境にあった場所を選択してください。

メモ 接続に失敗した場合は、5GHz/2.4GHzランプが点滅しますので、もう一度最初から接続をやり直してください。

設定手順（Windows XP/2000）

1 タスクトレイの アイコンを右クリックし、「プロファイルを表示する」をクリックします。

2 「WPS/AOSS」ボタンをクリックします。

3 画面にしたがって、本製品正面にあるAOSSボタンを5GHz/2.4GHzランプが点滅するまで(約3秒間)押し続けます。

メモ 本製品正面のAOSSボタンの代わりに、本製品の設定画面([詳細設定]－[無線設定]－[AOSS])にあるAOSSボタンを押して接続設定をすることもできます。

4 接続に成功すると、30秒～1分程度してから、「～完了しました」と表示されます。

※Windows XPの場合は、[完了]をクリックして、画面を閉じてください。

メモ 接続に失敗した場合は、5GHz/2.4GHzランプが点滅しますので、もう一度最初から接続をやり直してください。

以上で接続は完了です。

CLI設定手順

AOSS/WPS接続処理をCLIを使っておこなうには、以下のコマンドを入力します。

AOSS設定

```
(profile1)man$ airset aoss start
Do you really want to start AOSS, continue? (y/n)y
```

WPS設定

```
(profile1)man$ airset wps start
```

AOSS/WPSで無線接続できないときは...

AOSS/WPSで無線接続できないときは、以下の対策をおこなってください。

・本製品とパソコンとの距離が離れすぎていたり、壁や障害物等がある場合は、パソコンを本製品に近づけてからAOSS/WPS接続をおこなってください。

・他社製無線接続ツールがインストールされている場合は、削除した後、再度AOSS/WPS接続をおこなってください。

・セキュリティーソフトを一時的に停止してから、AOSS/WPS接続をおこなってください。AOSS/WPS接続が成功したらセキュリティーソフトを有効にしてください。

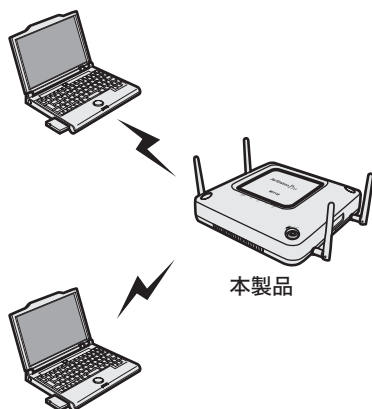
・無線LAN標準搭載パソコンをお使いの場合は、無線LAN機能がONになっているか、確認してください。

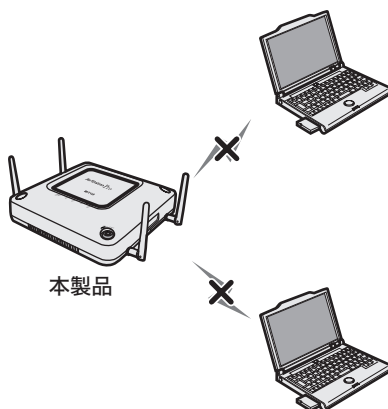
例2:プロファイラーを使用する(タイマー)

プロファイラー機能とは、プロファイルごとに本製品に設定可能なパラメーターを複数設定でき、自動もしくは手動で切り替えることができる機能です。この機能を使用することによって、時間帯によってユーザーを制限したり、通信を制限したりすることができます。

構成例

平日の昼間

本製品の無線機能が有効のため、
無線通信が可能

平日の夜間および休日

本製品の無線機能が無効のため、
無線通信が不可

条件

・平日の朝および昼間は本製品の無線機能をONにし、平日の夜間(23:00～30:00)と休日は本製品の無線機能をOFFにする。
・プロファイラー機能を使って、上記の切り替えが自動的におこなわれるように設定する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・クライアントパソコン

設定手順

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[管理設定]－[時刻]をクリックします。以下のように項目を設定して、[設定]をクリックします。

NTP機能　：使用する（チェックあり）
サーバー名：任意のNTPサーバーのIPアドレス（またはDNS解決可能なホスト名）
確認時間　：24時間毎

※ NTPサーバーを使用しない場合は、手動で日付や時刻を入力して[設定]をクリックしてください。

※ プロファイル機能有効時においても、本製品の内部時刻が正しくない場合（NTPサーバーもしくは手動で時刻が設定されていない状態）では、プロファイルの切り替えは開始されません。

4　画面左側の[管理設定]－[プロファイラ]をクリックします。[プロファイル情報の編集]をクリックします。

5　コピー元に「profile1」、コピー先に「profile2」を選択し[プロファイルをコピーする]をクリックします。「コピー先プロファイルの内容は上書きされます」と表示されたら、[設定]をクリックします。

プロファイルのコピーが終わったら、[編集を終了して前の画面へ戻る]をクリックします。

6 「現在のプロファイル」を「profile2」に変更して[設定]をクリックします。

7 画面左側の[無線設定]－[(802.11aの)無線基本]をクリックします。
「無線機能」の「使用する」のチェックを外して、[設定]をクリックします。

8 手順7と同様に、802.11gの無線機能を無効にします。

9 画面左側の[管理設定]－[プロファイラ]をクリックします。
「スケジュール一覧」の[タイムテーブルの編集]をクリックします。

10 「タイムテーブルの新規追加」で、平日の夜間に無線機能がOFFになるよう、下記のように設定して、[新規追加]をクリックします。

指定方法　　：曜日・時間で指定する
曜日　　　　：月～金を有効(チェックあり)、日と土を無効(チェックなし)
設定時間　　：23時00分～30時00分
プロファイル：profile2

プロファイラ設定 － タイムテーブルの編集　ヘルプ

編集を終了して前の画面へ戻る

タイムテーブルの新規追加　ヘルプ

指定方法	○日付で指定する　◉曜日・時間で指定する
年月日	-- 年 -- 月 -- 日
曜日	日 □　月 ☑　火 ☑　水 ☑　木 ☑　金 ☑　土 □
設定時間	23 時 00 分 ～ 30 時 00 分
プロファイルの選択	○プロファイルで指定する　○他の曜日の設定を使用する
プロファイル	profile2
曜日を指定	日

新規追加

11 手順10と同様に、「タイムテーブルの新規追加」で、休日に無線機能がOFFになるよう、下記のように設定して、[新規追加]をクリックします。

指定方法　　：曜日・時間で指定する
曜日　　　　：月～金を無効（チェックなし）、日と土を有効（チェックあり）
設定時間　　：06時00分～30時00分
プロファイル：profile2

設定が終わったら、[編集を終了して前の画面へ戻る]をクリックします。

12 「現在のプロファイル」で「profile1」を選択し、[設定]をクリックします。

13 「スケジューラ」で「有効(自動プロファイル切り替えモード)」を選択して、[設定]をクリックします。

※ スケジューラーを有効にした場合、本製品の設定変更ができなくなることがあります。
その場合は、いったんスケジューラーを無効にし、必要なプロファイルに切り替えてから設定を変更し、その後、スケジューラーを有効にしてください。

プロファイラ設定 ? ヘルプ

現在、スケジューラは無効です

スケジューラ	○ 無効(手動プロファイル切り替えモード) ◉ 有効(自動プロファイル切り替えモード)
現在のプロファイル	profile1

設定

スケジューラを有効にしても、NTPもしくは手動での時刻補正が実施されていない状態ではプロファイルの自動切り替えは開始されません。
時刻補正されるまでの間「管理プロファイル」が使用されます。

14 登録したスケジュールが「スケジュール一覧」と「タイムテーブル」に表示されていることを確認します。

以上で本製品の設定は完了です。

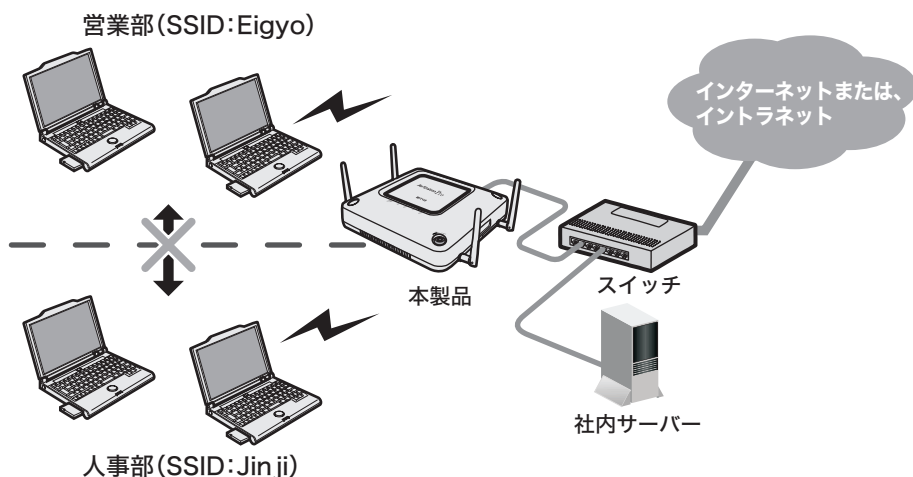
CLI設定手順

ここまでの設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
NTPサーバー(例:ntp.buffalo.jp)から時刻を自動取得する場合

(profile1)man$ setup ntp client enable server ntp.buffalo.jp
interval 24


手動で時刻(2011年12月31日12時34分56秒)を設定する場合

(profile1)man$ setup date 2011/12/31 12:34:56


(profile1)man$ edit start profnum 1
(profile1)man[edit]$ profile copy profname Profile1 to profname
Profile2 force
APXXXXXXXXXXXX
(profile1)
(profile1)man[edit]$ profile switch profname profile2 force
(profile2)man[edit]$ airset 11a wireless disable
(profile2)man[edit]$ airset 11g wireless disable
(profile2)man[edit]$ profile schedule add week weekdays from 23:00
to 30:00 profname profile2
(profile2)man[edit]$ profile schedule add week weekend from 6:00
to 30:00 profname profile2
(profile2)man[edit]$ profile switch profname profile1 force
(profile1)man[edit]$ profile schedule enable force


<再起動>


Hello!
APXXXXXXXXXXXX
Welcome to BUFFALO CLI
(profile1)man$
```

例3:部署間のセキュリティーを保ちたい(マルチSSID)

本製品は1台で複数の無線ネットワークを設定することができます。この機能を利用すると、あたかも複数台のエアステーションが設置されているかのようなネットワークを構築することができます。
ここでは例として、VLANを使用せずに簡易的にネットワークを分ける方法を説明します。

構成例

条件

・無線でインターネットに接続できる環境で、人事部と営業部など他部署間での無線通信に制限を設ける。(他部署間では無線通信を禁止する)※
※有線区間やプロキシ利用環境の場合を除きます。
・802.11a、802.11gともにメインの無線がすでに動作している。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

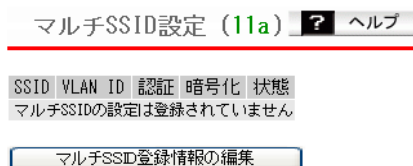
必要機器

・クライアントパソコン
・有線側ネットワーク機器(例:スイッチ、ルーターなど)

設定手順

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[無線設定]－[(使用する無線規格の)マルチSSID]をクリックし、[マルチSSID登録情報の編集]をクリックします。

4 **営業部の設定をおこないます。**
以下のように項目を設定して、[新規追加]をクリックします。

SSID	：	Eigyo
VLANID	：	1（変更なし）
無線の認証	：	WPA2-PSK
追加認証	：	追加認証を行わない
無線の暗号化	：	AES
WPA-PSK（事前共有キー）	：	abcdefgh（任意の値）、Key更新間隔：60（分）
ANY接続	：	許可する（チェックあり）
プライバシーセパレーター	：	SSIDセパレーター

5 **[設定]をクリックします。**

6 人事部の設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

SSID	:	Jinji
VLANID	:	1（変更なし）
無線の認証	:	WPA2-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	AES
WPA-PSK（事前共有キー）	:	ijklmnop（任意の値）、Key更新間隔：60（分）
ANY接続	:	許可する（チェックあり）
プライバシーセパレーター	:	SSIDセパレーター

7 [設定]をクリックします。

以上で本製品の設定は完了です。
無線パソコンからそれぞれのSSIDを使って、ネットワークへ接続してください。接続手順は、無線パソコンまたは無線子機のマニュアルを参照してください。

※ クライアントマネージャ3をお使いの場合は、プロファイルのインポート/エクスポート機能を使うと、複数のパソコンへの設定が簡単におこなえます。プロファイルのインポート/エクスポート機能については、クライアントマネージャ3のヘルプを参照してください。

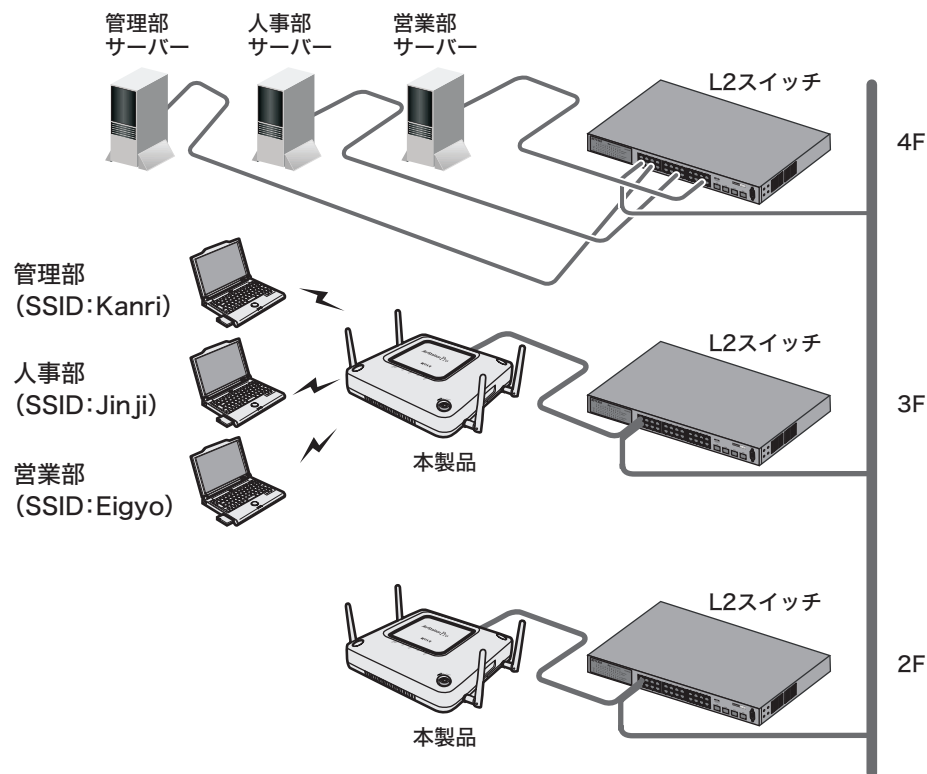
CLI設定手順

ここまでの設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11a ssid add ssidname Eigyo vlanid 1
auth wpa2psk cipher aes rekey 60 key abcdefgh
(profile1)man[edit]$ airset 11a ssid privacy ssidname Eigyo ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Eigyo enable
(profile1)man[edit]$ airset 11a ssid add ssidname Jinji vlanid 1
auth wpa2psk cipher aes rekey 60 key ijklmnop
(profile1)man[edit]$ airset 11a ssid privacy ssidname Jinji ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Jinji enable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

例4:部署間のセキュリティーを保ちたい(TagVLAN)

本製品は1台で複数の無線ネットワークを設定することができます。この機能を利用すると、あたかも複数台のエアステーションが設置されているかのようなネットワークを構築することができます。
ここでは例として、既存のVLANネットワークに本製品を追加する方法を説明します。

構成例

条件

・各階にTagVLANに対応したL2スイッチ(例:BS-G2024MR(別売))が導入されている。
・TagVLANを利用して、L2スイッチ同士を接続する。
・本製品の有線ポートとL2スイッチをTrunk接続する。
・本製品の管理をおこなう管理部と、本製品の管理VLANを統一する。
・各部署のサーバーにVLAN、SSIDを使用して接続できるようにする。
・他部署のサーバーやパソコンへは通信できないようにする。

使用機器

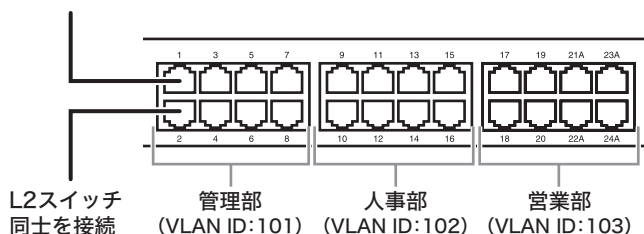
対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・クライアントパソコン
・有線側ネットワーク機器(例:TagVLANに対応したL2スイッチなど)

設定手順(L2スイッチ)

Webブラウザーを使って、ネットワークからL2スイッチへログインし、TagVLANの設定をおこないます。(ここでは例として、BS-G2024MR(別売)を使用します)

1 L2スイッチのマニュアルを参照して、L2スイッチの設定画面を表示します。

2 [詳細設定]-[VLAN設定]-[VLANステータス]をクリックします。

3 管理部のVLAN(101)を作成します。以下のように項目を設定して、[追加]をクリックします。

VLAN ID	：	101
VLAN名	：	Kanri
VLAN Management	：	チェックあり
ポート	：	1〜2を「Static Tagged」、3〜8を「Static Untagged」、9〜24を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged	U:Static Untagged	-:Not Member

新規VLAN 作成

VLAN ID:	101 (1-4094)
VLAN 名:	Kanri
VLAN Management:	☑

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static Tagged	◉	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	◉	◉	◉	◉	◉	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	○	○	○	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉

[設定] [再読込] [クリア]

4 **人事部のVLAN(102)を作成します。**
以下のように項目を設定して、[追加]をクリックします。

VLAN ID	：	102
VLAN名	：	Jinji
VLAN Management	：	チェックなし
ポート	：	1～2を「Static Tagged」、9～16を「Static Untagged」、3～8および17～24を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
101	T	T	U	U	U	U	U	U	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	Kanri
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged	U:Static Untagged	−:Not Member

5 営業部のVLAN(103)を作成します。以下のように項目を設定して、[追加]をクリックします。

VLAN ID	:	103
VLAN名	:	Eigyo
VLAN Management	:	チェックなし
ポート	:	1～2を「Static Tagged」、17～24を「Static Untagged」、3～16を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
101	T	T	U	U	U	U	U	U	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Kanri
102	T	T	–	–	–	–	–	–	U	U	U	U	U	U	U	U	–	–	–	–	–	–	–	–	Jinji
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged　U:Static Untagged　–:Not Member

新規VLAN 作成

VLAN ID:	103 (1–4094)
VLAN 名:	Eigyo
VLAN Management:	☐

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static Tagged	◉	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	◉
Not Member	○	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	○	○	○	○	○	○	○	○

[設定] [再読込] [クリア]

6 [詳細設定]－[VLAN設定]－[VLANポート設定]をクリックします。

7 各ポートにPVIDを設定します。以下のように項目を設定して、[設定]をクリックします。

ポート1～8	:	101
ポート9～16	:	102
ポート17～24	:	103

VLANポート設定

ポート	1	3	5	7	9	11	13	15	17	19	21	23
PVID	101	101	101	101	102	102	102	102	103	103	103	103
ポート	2	4	6	8	10	12	14	16	18	20	22	24
PVID	101	101	101	101	102	102	102	102	103	103	103	103

[設定] [再読込]

8 [詳細設定]－[VLAN設定]－[VLANステータス]をクリックします。

9 VLANステータスに表示されているVLAN1の欄にある[編集]をクリックします。

10 VLAN1に所属するポートをすべて「Not Member」に設定します。以下のように項目を設定して、[設定]をクリックします。

VLAN ID　：　1
VLAN名　：　空欄
VLAN Management　：　チェックなし
ポート　：　1～24を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
101	T	T	U	U	U	U	U	U	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
102	T	T	－	－	－	－	－	－	U	U	U	U	U	U	U	U	－	－	－	－	－	－	－	－
103	T	T	－	－	－	－	－	－	－	－	－	－	－	－	－	－	U	U	U	U	U	U	U	U
PVID	101	101	101	101	101	101	101	101	102	102	102	102	102	102	102	102	103	103	103	103	103	103	103	103

T:Static Tagged　U:Static Untagged　－:Not Member

新規VLAN 作成

VLAN ID:	1 (1-4094)
VLAN 名:	
VLAN Management:	☐

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉

[設定] [再読込] [クリア]

以上でL2スイッチの設定は完了です。
続いて、本製品の設定をおこないます。

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、VLANおよびマルチSSIDの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[無線設定]－[(使用する無線規格の)マルチSSID]をクリックし、[マルチSSID登録情報の編集]をクリックします。

4 管理部の設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

SSID	：	Kanri
VLAN ID	：	101
無線の認証	：	WPA2-PSK
追加認証	：	追加認証を行わない
無線の暗号化	：	AES
WPA-PSK(事前共有キー)	：	abcdefgh(任意の値)、Key更新間隔:60(分)
ANY接続	：	許可する(チェックあり)
プライバシーセパレーター	：	SSIDセパレーター

5 [設定]をクリックします。

6 人事部の設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

SSID	:	Jinji
VLAN ID	:	102
無線の認証	:	WPA2-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	AES
WPA-PSK(事前共有キー)	:	ijklmnop(任意の値)、Key更新間隔:60(分)
ANY接続	:	許可する(チェックあり)
プライバシーセパレーター	:	SSIDセパレーター

7 [設定]をクリックします。

8 営業部の設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

SSID	：	Eigyo
VLAN ID	：	103
無線の認証	：	WPA2-PSK
追加認証	：	追加認証を行わない
無線の暗号化	：	AES
WPA-PSK(事前共有キー)	：	qrstuvwx(任意の値)、Key更新間隔:60(分)
ANY接続	：	許可する(チェックあり)
プライバシーセパレーター	：	SSIDセパレーター

9 [設定]をクリックします。

10 画面左側の[LAN設定]－[VLAN設定]をクリックします。

11 **管理VLANと有線ポートのVLAN設定を以下のように変更して、[設定]をクリックします。**

管理VLAN ID ： 101
VLANモード ： Tagged Port

VLANモード・ID設定 ? ヘルプ

インターフェース VLAN

インターフェース	VLANモード	VLAN ID
有線ポート(#1)	Tagged Port	1
無線基本ポート(11a) SSID[XXXXXXXXXXXX_A]	Untagged Port	1
無線マルチSSID(11a) SSID[Kanri]	Untagged Port	101
無線マルチSSID(11a) SSID[Jinji]	Untagged Port	102
無線マルチSSID(11a) SSID[Eigyo]	Untagged Port	103
無線基本ポート(11g) SSID[XXXXXXXXXXXX_G]	Untagged Port	1

サブネット VLAN

サブネット名	サブネット種別	VLAN ID
Management	管理サブネット	101

[設定]

以上で本製品の設定は完了です。
本書のP24の図に合わせて、本製品とL2スイッチ、およびL2スイッチ同士を接続してください。
また、無線パソコンからそれぞれのSSIDを使って、ネットワークへ接続してください。接続手順は、無線パソコンまたは無線子機のマニュアルを参照してください。

※ クライアントマネージャ3をお使いの場合は、プロファイルのインポート/エクスポート機能を使うと、複数のパソコンへの設定が簡単におこなえます。プロファイルのインポート/エクスポート機能については、クライアントマネージャ3のヘルプを参照してください。

CLI設定手順

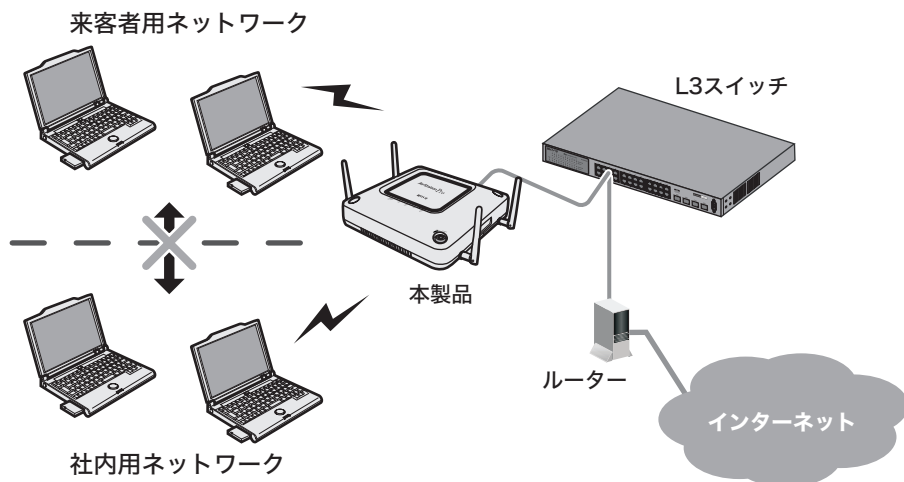
ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11a ssid add ssidname Kanri vlanid 101
auth wpa2psk cipher aes rekey 60 key abcdefgh
(profile1)man[edit]$ airset 11a ssid privacy ssidname Kanri ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Kanri enable
(profile1)man[edit]$ airset 11a ssid add ssidname Jinji vlanid 102
auth wpa2psk cipher aes rekey 60 key ijklmnop
(profile1)man[edit]$ airset 11a ssid privacy ssidname Jinji ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Jinji enable
(profile1)man[edit]$ airset 11a ssid add ssidname Eigyo vlanid 103
auth wpa2psk cipher aes rekey 60 key qrstuvwx
(profile1)man[edit]$ airset 11a ssid privacy ssidname Eigyo ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Eigyo enable
(profile1)man[edit]$ ip lan vlan 101 force
(profile1)man[edit]$ ether port 1 vlan mode tagged
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

例5:来客用フリースポットの設置(TagVLAN)

本製品は1台で複数の無線ネットワークを設定することができます。この機能を利用すると、あたかも複数台のエアステーションが設置されているかのようなネットワークを構築することができます。
ここでは例として、本製品を社内の無線アクセスポイント兼来客用フリースポットアクセスポイントとして使用する方法を説明します。

構成例

条件

・ハードウェアIPフィルターに対応したL3スイッチ(例:BS-G3024MR(別売))が導入されている。
・TagVLANを利用して、本製品とL3スイッチを接続する。
・来客用フリースポットとして使用できるように本製品を設定する。
・来客用フリースポットからは、社内ネットワークにアクセスできないようにする。

使用機器

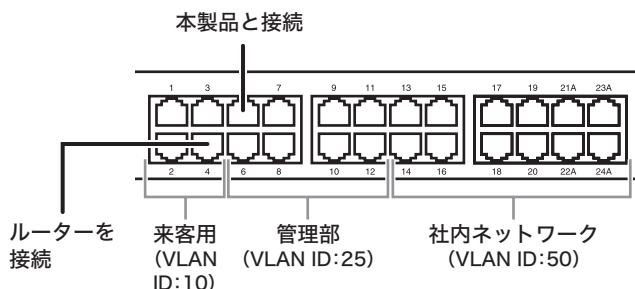
対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・クライアントパソコン
・有線側ネットワーク機器(例:ハードウェアIPフィルターに対応したL3スイッチ、ルーターなど)

設定手順(L3スイッチのVLAN設定)

Webブラウザーを使って、ネットワークからL3スイッチへログインし、TagVLANの設定をおこないます。(ここでは例として、BS-G3024MR(別売)を使用します)

1 L3スイッチのマニュアルを参照して、L3スイッチの設定画面を表示します。

2 [基本設定]−[VLAN・IP設定]−[VLAN・IPステータス]をクリックします。

3 来客用(FreeSpot)のVLAN(10)を作成します。
以下のように項目を設定して、[追加]をクリックします。

VLAN ID　：10
VLAN名　：FreeSpot
IPアドレス　：192.168.10.254
サブネットマスク　：255.255.255.0/24
ポート　：1〜4を「Static Untagged」、5を「Static Tagged」、6〜26を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged　U:Static Untagged　−:Not Member

新規VLAN 作成

VLAN ID:	10 (1-4094)
VLAN 名:	FreeSpot
IPアドレス:	192.168.10.254
サブネットマスク:	255.255.255.0/24

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	○	○	○	○	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	◉	◉	◉	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉

[設定] [再読込] [クリア]

4 管理部のVLAN(25)を作成します。
以下のように項目を設定して、[追加]をクリックします。

VLAN ID　：25
VLAN名　：Kanri
IPアドレス　：192.168.11.254
サブネットマスク　：255.255.255.0/24
ポート　：5を「Static Tagged」、6～12および25～26を「Static Untagged」、1～4および13～24を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
10	U	U	U	U	T	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	FreeSpot
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged　U:Static Untagged　–:Not Member

新規VLAN 作成

VLAN ID:	25 (1–4094)
VLAN 名:	Kanri
IPアドレス:	192.168.11.254
サブネットマスク:	255.255.255.0/24

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	○	○	○	○	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	○	○	○	○	○	○	○	○	○	○	○	○	◉	◉
Not Member	◉	◉	◉	◉	○	○	○	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	○	○

[設定] [再読込] [クリア]

5 社内ネットワークのVLAN(50)を作成します。
以下のように項目を設定して、[追加]をクリックします。

VLAN ID　：50
VLAN名　：Shanai
IPアドレス　：192.168.50.254
サブネットマスク　：255.255.255.0/24
ポート　：5を「Static Tagged」、13～24を「Static Untagged」、1～4および6～12を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
10	U	U	U	U	T	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	FreeSpot
25	–	–	–	–	T	U	U	U	U	U	U	U	–	–	–	–	–	–	–	–	–	–	–	–	U	U	Kanri
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged　U:Static Untagged　–:Not Member

新規VLAN 作成

VLAN ID:	50 (1–4094)
VLAN 名:	Shanai
IPアドレス:	192.168.50.254
サブネットマスク:	255.255.255.0/24

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	○	○	○	○	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	○	○	○	○	○	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	○	○
Not Member	◉	◉	◉	◉	○	◉	◉	◉	◉	◉	◉	◉	○	○	○	○	○	○	○	○	○	○	○	○	◉	◉

設定　再読込　クリア

6 [基本設定]－[VLAN･IP設定]－[VLANポート設定]をクリックします。

7 各ポートにPVIDを設定します。
以下のように項目を設定して、[設定]をクリックします。

ポート1～4　：10
ポート5～12および25～26　：25
ポート13～24　：50

VLANポート設定

ポート	1	3	5	7	9	11	13	15	17	19	21	23	25
PVID	10	10	25	25	25	25	50	50	50	50	50	50	25
ポート	2	4	6	8	10	12	14	16	18	20	22	24	26
PVID	10	10	25	25	25	25	50	50	50	50	50	50	25

設定　再読込

8 [基本設定]－[VLAN･IP設定]－[VLAN･IPステータス]をクリックします。

9 VLANステータスに表示されているVLAN 1の欄にある[編集]をクリックします。

10 VLAN 1に所属するポートをすべて「Not Member」に設定します。
以下のように項目を設定して、[設定]をクリックします。

VLAN ID ： 1
VLAN名 ： 空欄
IPアドレス ： 192.168.1.254
サブネットマスク ： 255.255.255.0/24
ポート ： 1～26を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
10	U	U	U	U	T	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	FreeSpot
25	–	–	–	–	T	U	U	U	U	U	U	U	–	–	–	–	–	–	–	–	–	–	–	–	U	U	Kanri
50	–	–	–	–	T	–	–	–	–	–	–	–	U	U	U	U	U	U	U	U	U	U	U	U	–	–	Shanai
PVID	10	10	10	10	25	25	25	25	25	25	25	25	50	50	50	50	50	50	50	50	50	50	50	50	25	25	

T:Static Tagged　U:Static Untagged　–:Not Member

新規VLAN 作成

VLAN ID:	1 (1–4094)
VLAN 名:	
IPアドレス:	192.168.1.254
サブネットマスク:	255.255.255.0/24

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉

[設定] [再読込] [クリア]

以上でL3スイッチのVLAN設定は完了です。
続いて、L3スイッチのハードウェアIPフィルター設定をおこないます。

設定手順(L3スイッチのハードウェアIPフィルター設定)

RS-232C(コンソール)接続でL3スイッチへログインし、ハードウェアIPフィルターの設定をおこないます。(ここでは例として、BS-G3024MR(別売)を使用します)

1 L3スイッチと設定用パソコンを、RS-232Cケーブルで接続します。

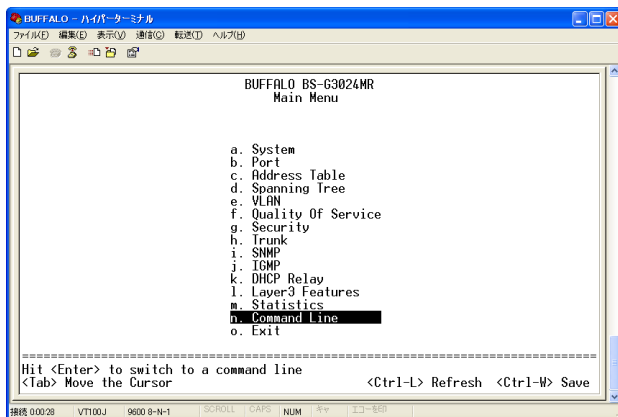
2 ターミナルソフトを次のとおりに設定し、L3スイッチにアクセスします。

- 接続方法:COM1など
- データレート:9600bps
- データビット:8
- ストップビット:1
- パリティ:なし
- フロー制御:なし
- エミュレーション設定:VT100(または自動検出)
- キーの使いかた(ハイパーターミナル使用時):ターミナルキー

3 ターミナルが適切にセットアップできたら、ログインメニューが表示されます。
文字が表示されない場合は<Enter>を押してください。

4 Login:にadminと入力し、<Enter>を押します。

5 Password:に、L3スイッチに設定されているパスワードを入力し、<Enter>を押します。
(BS-G3024MRの場合、初期設定ではパスワードは設定されていません)

6 以下のメニュー画面が表示されたら、<n>を押します。
<n>を押すと、CLIモードに切り替わります。

7 Global Configurationコマンドモードに入ります。

```
BS-G3024MR# configure
Configuring from terminal....
BS-G3024MR(config)#
```

8 「buffalo1」というアクセスリストを登録します。

```
BS-G3024MR(config)# access-list buffalo1
BS-G3024MR(config-access)#
```

9 アクセスリスト(buffalo1)に、来客用ネットワーク(192.168.10.0/24)から社内ネットワーク(192.168.50.0/24)へのアクセスを禁止する内容を登録します。

```
BS-G3024MR(config-access)# deny 192.168.10.0/24 192.168.50.0/24
BS-G3024MR(config-access)#
```

10 アクセスリスト(buffalo1)に、社内ネットワーク(192.168.50.0/24)から来客用ネットワーク(192.168.10.0/24)へのアクセスを禁止する内容を登録します。

```
BS-G3024MR(config-access)# deny 192.168.50.0/24 192.168.10.0/24
BS-G3024MR(config-access)#
```

11 Global Configurationコマンドモードに戻ります。

```
BS-G3024MR(config-access)# exit
BS-G3024MR(config)#
```

12 Interface Configurationコマンドモードに入り、ポート5の設定を開始します。

```
BS-G3024MR(config)# interface ethernet 5
BS-G3024MR(config-if)#
```

13 手順8～10で作成したアクセスリスト（buffalo1）の内容を、ポート5に適用します。

```
BS-G3024MR(config-if)# ip access-list buffalo1 inbound
BS-G3024MR(config-if)#
```

14 Global Configurationコマンドモードに戻ります。

```
BS-G3024MR(config-if)# exit
BS-G3024MR(config)#
```

15 ここまでの設定内容を保存します。

```
BS-G3024MR(config)# system save

 Saving Configuration ...

Configuration saved to NVRAM
BS-G3024MR(config)#
```

16 exitコマンドを入力し、ログアウトします。

```
BS-G3024MR(config)# exit
BS-G3024MR# exit
```

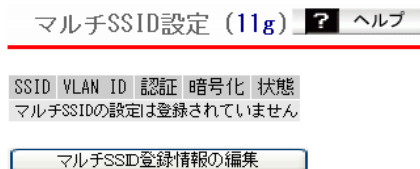
以上でL3スイッチのハードウェアIPフィルター設定は完了です。
続いて、本製品の設定をおこないます。

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、TagVLANおよびマルチSSIDの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[無線設定]－[(802.11gの)マルチSSID]をクリックし、[マルチSSID登録情報の編集]をクリックします。

4 来客用ネットワークの設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

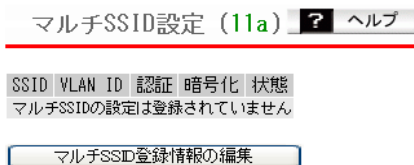
SSID ： FreeSpot
VLANID ： 10
無線の認証 ： WPA2-PSK
追加認証 ： 追加認証を行わない
無線の暗号化 ： AES
WPA-PSK（事前共有キー） ： freespot（任意の値）、Key更新間隔：60（分）
ANY接続 ： 許可する（チェックあり）
プライバシーセパレーター ： STAセパレーター

5 [設定]をクリックします。

6 画面左側の[無線設定]ー[(802.11aの)マルチSSID]をクリックし、[マルチSSID登録情報の編集]をクリックします。

マルチSSID設定（11a） ? ヘルプ

SSID	VLAN ID	認証	暗号化	状態
マルチSSIDの設定は登録されていません				

マルチSSID登録情報の編集

7 社内ネットワークの設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

SSID	：	shanai
VLANID	：	50
無線の認証	：	WPA2-PSK
追加認証	：	追加認証を行わない
無線の暗号化	：	AES
WPA-PSK(事前共有キー)	：	buffalo-shanai(任意の値)、Key更新間隔:60(分)
ANY接続	：	許可する(チェックあり)
プライバシーセパレーター	：	SSIDセパレーター

8 [設定]をクリックします。

9 [LAN設定]－[VLAN設定]をクリックします。

10 VLANの設定をおこないます。
以下のように項目を設定して、[設定]をクリックします。

有線ポート　：Tagged Port
無線基本ポート(11a)　：VLAN ID 25
無線マルチSSID(11a)　：VLAN ID 50
無線基本ポート(11g)　：VLAN ID 25
無線マルチSSID(11g)　：VLAN ID 10
管理VLAN ID　：25

以上で本製品の設定は完了です。
本書のP36の図に合わせて、本製品とL3スイッチを接続してください。
また、無線パソコンからそれぞれのSSIDを使って、ネットワークへ接続してください。接続手順は、無線パソコンまたは無線子機のマニュアルを参照してください。

※ クライアントマネージャ3をお使いの場合は、プロファイルのインポート/エクスポート機能を使うと、複数のパソコンへの設定が簡単におこなえます。プロファイルのインポート/エクスポート機能については、クライアントマネージャ3のヘルプを参照してください。

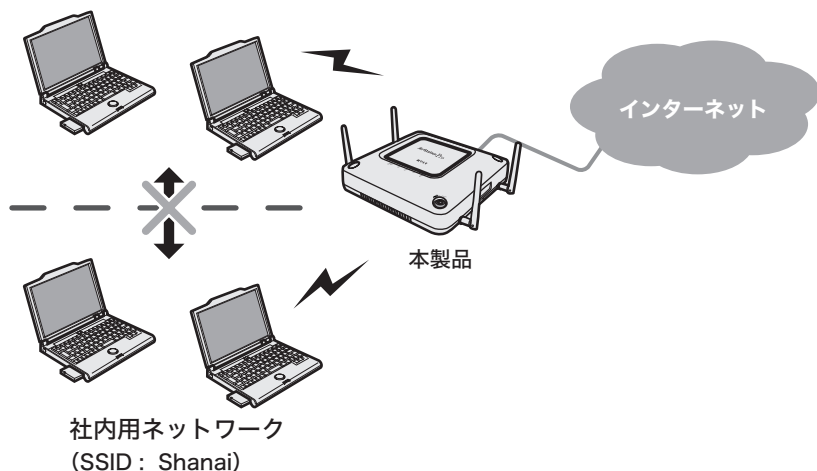
CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11g ssid add ssidname FreeSpot vlanid 10
auth wpa2psk cipher aes rekey 60 key freespot
(profile1)man[edit]$ airset 11g ssid privacy ssidname FreeSpot
station
(profile1)man[edit]$ airset 11g ssid anyscan ssidname FreeSpot
enable
(profile1)man[edit]$ airset 11a ssid add ssidname Syanai vlanid 50
auth wpa2psk cipher aes rekey 60 key buffalo-syanai
(profile1)man[edit]$ airset 11a ssid privacy ssidname Syanai ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Syanai enable
(profile1)man[edit]$ ip lan vlan 25 force
(profile1)man[edit]$ ether port 1 vlan mode tagged
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

例6:来客用フリースポットの設置(簡易ルーター機能)

本製品は簡易ルーター機能を搭載しています。この機能を利用することでルーターを別途用意することなく、本製品1台で社内用無線アクセスポイントと来客用フリースポットを設定できます。ここでは例として、本製品を社内の無線アクセスポイント兼来客用フリースポットアクセスポイントとして使用する方法を説明します。

構成例

条件

・来客用フリースポットとして使用できるように本製品を設定する。
・来客用フリースポットからは、社内ネットワークにアクセスできないようにする。
・小規模での運用を想定。
・インターネット接続方法としてPPPoEを使用する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

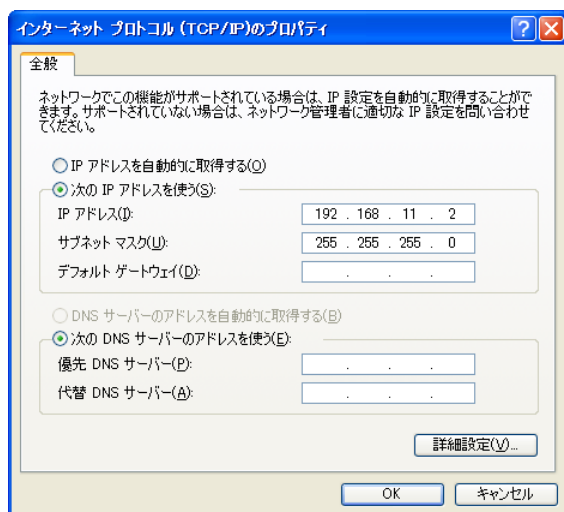
・AOSSに対応した設定用パソコン

※ 設定用パソコンには、あらかじめクライアントマネージャV(Windows 7/Vistaの場合)またはクライアントマネージャ3(Windows XP/2000/Me/98SEの場合)がインストールされている必要があります。

設定手順（設定用パソコンの設定）

設定用パソコンのIPアドレスを固定し、設定用パソコンと本製品をAOSS接続します。

1 **設定用パソコンのIPアドレスを固定にします。**
以下のように設定して、[OK]をクリックします。
（以下は、Windows XPの場合の画面です）

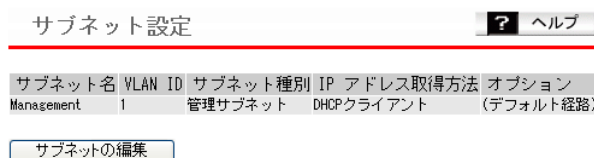
「次のIPアドレスを使う」
IPアドレス　：　192.168.11.2
サブネットマスク　：　255.255.255.0
デフォルトゲートウェイ：　空欄
「次のDNSサーバーのアドレスを使う」
優先DNSサーバー　：　空欄
代替DNSサーバー　：　空欄

2 **「例1：AOSS/WPSを使って本製品と無線接続する」（P4）を参照して、本製品と設定用パソコンをAOSSで接続します。**

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、TagVLANおよびマルチSSIDの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[LAN設定]－[サブネット設定]をクリックします。
[サブネットの編集]をクリックします。

4 「サブネットの表示/操作」に登録されている「Management」欄の[編集]をクリックします。

サブネットの表示/操作 ? ヘルプ

サブネット名	VLAN ID	サブネット種別	IPアドレス取得方法	デフォルト経路	操作
Management	1	管理サブネット	DHCPクライアント	◉	[編集]

[設定]

5 管理用サブネット（Management）を以下のように設定して、[修正保存]をクリックします。

サブネット名 ： Shanai
サブネット種別 ： 管理サブネット
VLAN ID ： 1
IPアドレスの取得方法 ： 手動設定 192.168.11.100
IPアドレス ： 192.168.11.100（255.255.255.0）
ルーティング ： ルーティング
デフォルトゲートウェイ ： 空欄
DNS ： 空欄
動的経路 ： 受信「RIPv1」と「RIPv2」にのみチェックマークを付ける
UPnP IGD ： 使用しない
MTU ： 1500
DHCPサーバー ： サブネットにDHCPサーバー機能を提供する
割り当てIPアドレス ： 192.168.11.10から30台

サブネット情報の編集 ? ヘルプ

サブネット名	Shanai
サブネット種別	◉管理サブネット
VLAN ID	1
IP アドレスの取得方法	◉ 手動設定 ○ DHCP クライアント
IP アドレス	IP アドレス 192.168.11.100 サブネットマスク 255.255.255.0
ルーティング	ルーティング
デフォルトゲートウェイ	手動設定
DNS	プライマリーサーバー: セカンダリーサーバー:
動的経路	送信 ： ☐RIPv1 ☐RIPv2 受信 ： ☑RIPv1 ☑RIPv2
UPnP IGD	使用しない
MTU	1500
DHCP サーバー	○使用しない ◉サブネットにDHCPサーバー機能を提供する ○サブネットにDHCPサーバー機能をRelayする 割り当て IP アドレス 192.168.11.10 から 30 台 除外アドレス

修正保存

6 [設定]をクリックします。

7 同様に、サブネットの編集画面で、来客用フリースポットのサブネットを追加します。

サブネット名	：	FreeSpot
サブネット種別	：	LANサブネット
VLAN ID	：	2
IPアドレスの取得方法	：	手動設定
IPアドレス	：	192.168.12.1（255.255.255.0）
ルーティング	：	ルーティング
デフォルトゲートウェイ	：	空欄
DNS	：	空欄
動的経路	：	受信「RIPv1」と「RIPv2」にのみチェックマークを付ける
UPnP	：	使用しない
MTU	：	1500
DHCPサーバー	：	サブネットにDHCPサーバー機能を提供する
割り当てIPアドレス	：	192.168.12.10から30台

サブネット情報の編集 ? ヘルプ

サブネット名	FreeSpot
サブネット種別	◉LAN サブネット ○Internet サブネット
VLAN ID	2
IP アドレスの取得方法	◉ 手動設定 ○ DHCP クライアント
IP アドレス	IP アドレス 192.168.12.1 サブネットマスク 255.255.255.0
ルーティング	ルーティング
デフォルトゲートウェイ	手動設定
DNS	プライマリーサーバー: セカンダリーサーバー:
動的経路	送信： ☐RIPv1 ☐RIPv2 受信： ☑RIPv1 ☑RIPv2
UPnP IGD	使用しない
MTU	1500
DHCP サーバー	○使用しない ◉サブネットにDHCPサーバー機能を提供する ○サブネットにDHCPサーバー機能をRelayする 割り当て IP アドレス 192.168.12.10 から 30 台 除外アドレス

新規追加

8 画面左側の[無線設定]－[(802.11aの)マルチSSID]をクリックします。[マルチSSID登録情報の編集]をクリックします。

マルチSSID設定（11a） ? ヘルプ

SSID	VLAN ID	認証	暗号化	状態
マルチSSIDの設定は登録されていません				

マルチSSID登録情報の編集

9 社内ネットワークのSSID設定を以下のように設定して、[新規追加]をクリックします。

SSID	：	Shanai
VLANID	：	1
無線の認証	：	WPA/WPA2 mixedmode-PSK
追加認証	：	追加認証を行わない
無線の暗号化	：	TKIP/AES mixed
WPA-PSK（事前共有キー）	：	abcdefgh（8～63文字の任意の値）
Key更新間隔	：	60分
ANY接続	：	許可する
プライバシーセパレーター	：	SSIDセパレーター

10 [設定]をクリックします。

11 画面左側の[無線設定]－[(802.11gの)マルチSSID]をクリックします。
[マルチSSID登録情報の編集]をクリックします。

マルチSSID設定（11g） ? ヘルプ

SSID	VLAN ID	認証	暗号化	状態
マルチSSIDの設定は登録されていません				

マルチSSID登録情報の編集

12 来客用フリースポットのSSID設定を以下のように設定して、[新規追加]をクリックします。

SSID	：	FreeSpot
VLANID	：	2
無線の認証	：	WPA/WPA2mixedmode-PSK
追加認証	：	追加認証を行わない
無線の暗号化	：	TKIP/AESmixed
WPA-PSK（事前共有キー）	：	ijklmnop（8～63文字の任意の値）
Key更新間隔	：	60分
ANY接続	：	許可する
プライバシーセパレーター	：	STAセパレーター

13 [設定]をクリックします。

14 画面左側の[TOP]をクリックします。

15 TOP画面の「インターネット接続を設定する」をクリックします。

16 VLANモードを設定します。以下のように項目を設定して、[進む]をクリックします。

VLANモード　：UntaggedPort

17 「PPPoEクライアント機能を使用する」をクリックします。

18 インターネット回線の接続先情報を設定します。以下のように項目を設定して、[進む]をクリックします。

接続ユーザー名　：ご契約のプロバイダー指定のユーザー名
接続パスワード　：ご契約のプロバイダー指定のパスワード

インターネット接続を設定する
インターネット回線の接続設定（PPPoE）

インターネット接続のために必要な情報を入力します。

接続ユーザー名	xxxxxxxx@xxx.xxx.xxx.xxx
接続パスワード	●●●●●●●● ●●●●●●●●（確認用）

戻る　進む

19 設定内容を確認し、[接続開始]をクリックします。

サブネット名	Internet-Subnet
サブネット種別	Internet サブネット
VLAN ID	4094
IP アドレスの取得方法	PPPoE クライアント
PPPoE	接続先ユーザー名： xxxxxx@xxx.xxx.xxx.xxx 接続先パスワード： ******** サービス名 ： キープアライブ ： on
ルーティング	アドレス変換(NAPT)
DNS	通知されたDNSを使用する
動的経路	送信: 使用しない 受信: RIPv1,RIPv2
MTU	1454

20 本製品が接続設定を確認しますので、画面が切り替わるまでしばらく待ちます。

21 以下の画面が表示されたら接続設定は完了です。
[完了]をクリックしてください。

22 手順1で変更した設定用パソコンのIPアドレス設定を元の設定に戻します。

以上で本製品の設定は完了です。

CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$ airset 11g ssid add ssidname FreeSpot vlanid 2
auth wpa2mixedpsk cipher mixed rekey 60 key abcdefgh
(profile1)man[edit]$ airset 11g ssid privacy ssidname FreeSpot
station
(profile1)man[edit]$ airset 11g ssid anyscan ssidname FreeSpot
enable
(profile1)man[edit]$ airset 11a ssid add ssidname Shanai vlanid 1
auth wpa2mixed cipher mixed rekey 60 key ijklmnop
(profile1)man[edit]$ airset 11a ssid privacy ssidname Shanai ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Shanai enable
(profile1)man[edit]$ ip subnet name Management address
192.168.11.100/24
(profile1)man[edit]$ ip dhcp-server lease name Management mode
server from 192.168.11.10 num 30
(profile1)man[edit]$ ip subnet rename name Management Shanai
(profile1)man[edit]$ ip subnet add name FreeSpot type lan vlan 2
address 192.168.12.1/24
(profile1)man[edit]$ ip dhcp-server lease name FreeSpot mode server
from 192.168.12.10 num 30
(profile1)man[edit]$ ip subnet add name Internet type inet vlan 4094
address pppoe user [PPPoE接続ユーザー名] pass [PPPoE接続パスワード] link
alltime keepalive lcp
(profile1)man[edit]$ ip routing subnet name Internet forwarding
enable napt outbound
(profile1)man[edit]$ ip defaultgw name Internet
(profile1)man[edit]$ ether port 1 vlan mode untagged vlan 4094
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

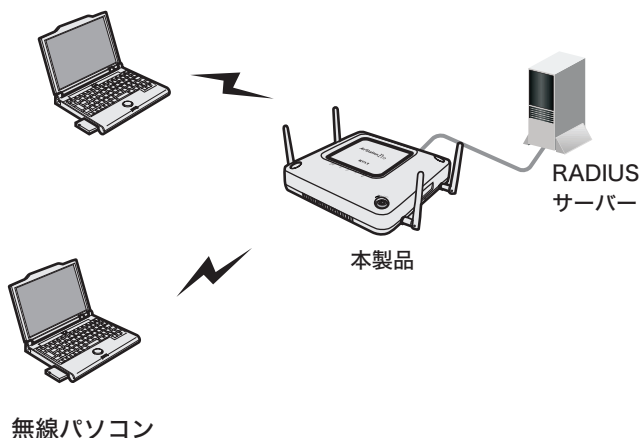
例7:802.1X無線認証を利用する(MACアドレスによる制限の場合)

本製品はRADIUSサーバーを用いた無線パソコン認証に対応しており、強固なセキュリティーを持つ無線ネットワークを構築することができます。RADIUSサーバーを利用した認証方式には次のものがあり、パソコンの対応状況によって使い分けることができます。

- •MAC-RADIUS認証　：すべてのパソコンで利用可能
- •IEEE802.1X/EAP認証　：IEEE802.1X/EAP準拠で、動的WEPキー配信をサポートしたパソコンで利用可能
- •WPA-EAP認証　：WPA-EAP(Enterprise)に対応したパソコンで利用可能
- •WPA2-EAP認証　：WPA2-EAP(IEEE802.11i)に対応したパソコンで利用可能

ここでは例として、RADIUSサーバーにMicrosoft Windows Server 2003搭載の認証サーバー(インターネット認証サービス)を使用する場合の手順を説明します。

暗号化の種別	セキュリティー強度	サプリカント	RADIUSサーバーの対応
MAC-RADIUS	△	不要	PAP対応
IEEE802.1X/EAP	○	必要	EAP対応
WPA-EAP WPA2-EAP WPA/WPA2 EAP	◎		

構成例

条件

・RADIUSサーバーには、インターネット認証サービス（IAS）が正常にインストールされ、認証サービスが動作している。
（インターネット認証サービスやRADIUSサーバーの設定などの詳細は、市販の書籍や各サーバーのマニュアルなどをご参照ください）
・接続をおこなうすべてのパソコンにサプリカントがインストールされ、必要な設定がおこなわれている。
（サプリカントのインストールや設定は、各ソフトウェアのマニュアルをご参照ください。
弊社製無線子機をお使いの場合、添付のクライアントマネージャ3のヘルプをご参照ください）

使用機器

対象機器

本製品（WAPM-APG300N/WAPM-AG300N）

必要機器

・RADIUSサーバー（Windows Server 2003）
・クライアントパソコン

設定手順（本製品）

Webブラウザーを使って、本製品の設定画面へログインし、認証の設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「無線LANの暗号化を設定する（RADIUSサーバーを使う）」をクリックします。

3 「11aと11gに共通の暗号化を設定する」をクリックします。

※ 選択した規格の無線ポートのみ設定されます。選択されなかった無線規格については、認証・暗号化設定をおこないません。

4 使用する暗号化方式をクリックします。

※ 接続する無線機器のすべてがサポート可能な暗号化方式を選択します。MAC-RADIUS認証については、RADIUSサーバーが対応している必要があります。

・MAC-RADIUS認証を選択する場合は、次の画面が表示されますので任意のWEP暗号化キーを入力してください。

5 RADIUSサーバー名とSharedSecretを入力して、[進む]をクリックします。

※ ここで入力したSharedSecretは、RADIUSサーバー側にも同じ値を設定します。

6 [設定]をクリックします。

7 [設定完了]をクリックします。

以上で本製品の設定は完了です。
続いてRADIUSサーバーの設定をおこないます。

CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

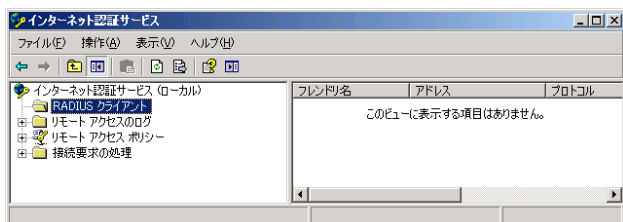
```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$


MAC-RADIUS 認証の場合

(profile1)man[edit]$ airset 11a ssid security ssidnum 1 auth
none cipher wep fixed keytype ascii128 transmit 1 key abcdefghijklm
(profile1)man[edit]$ airset 11a ssid addsecurity ssidnum 1 mode
macradius authmac


IEEE802.1X/EAP 認証の場合

(profile1)man[edit]$ airset 11a ssid security ssidnum 1 auth
eap cipher wep rekey 60 key 128 addkey disable


WPA/WPA2-EAP 認証の場合
(profile1)man[edit]$ airset [11a ssid security ssidnum 1 auth
[wpaeap | wpa2eap | wpa2mixedeap] cipher aes rekey 60


(profile1)man[edit]$ radius primary enable server (RADIUS サーバー名)
secret (SharedSecret)
(profile1)man[edit]$ airset [11a | 11g] wireless enable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

設定手順(RADIUSサーバー)

RADIUSサーバーへログインし、本製品を登録します。

1 RADIUSサーバー(Microsoft Windows Server 2003)にログインします。

2 スタートメニューから[コントロールパネル]−[管理ツール]−[インターネット認証サービス]をクリックします。

3 「RADIUSクライアント」を選択します。

4 ウィンドウ右側の空白部分を右クリックし、表示されたメニューから[新規作成]−[RADIUSクライアント]を選択します。

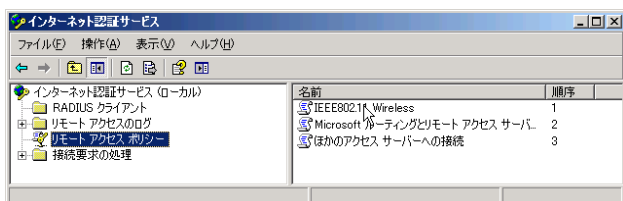
5 「名前とアドレス」設定で、「フレンドリ名」と「クライアントのアドレス」を設定し、[次へ]をクリックします。

※ フレンドリ名には本製品を示す任意の名前を、クライアントのアドレスには、本製品のIPアドレス(またはホスト名)を入力してください。

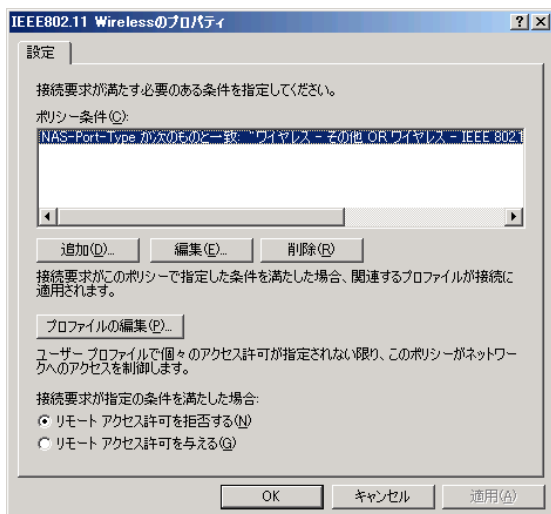
6 「追加情報」設定で、「クライアントベンダ」・「共有シークレット」を入力します。

※ クライアントベンダには「RADIUS Standard」を、共有シークレットには本製品に設定した「Shared Secret」を入力してください。

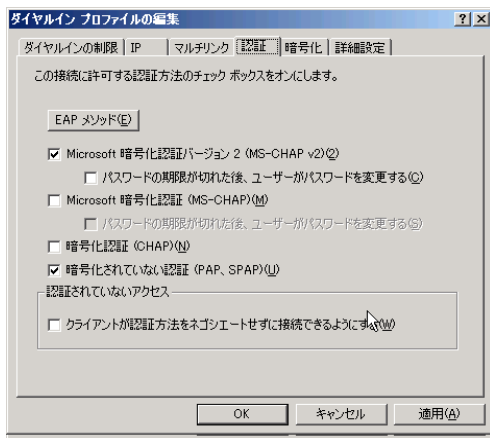
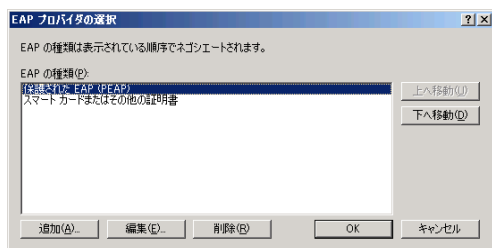
7 [完了]をクリックします。

8 「リモートアクセスポリシー」を選択します。

9 ウィンドウ右側から無線認証に使用するプロファイルを選択します。右クリックします。

10 選択した項目を右クリックし、[プロパティ]を選択します。

11 [プロファイルの編集]をクリックします。

12 [認証]タブをクリックします。

13 認証の設定をおこないます。

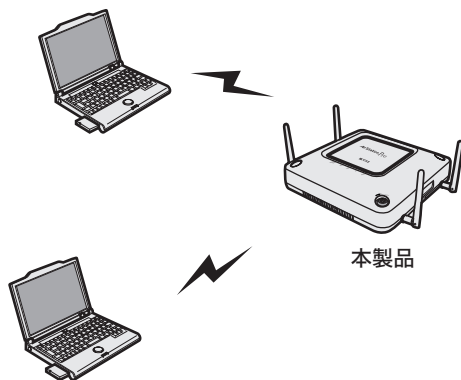
・認証にMAC-RADIUSを使用する場合は、「暗号化されていない認証（PAP、SPAP）」にチェックマークをつけて、[OK]をクリックします。

・認証にEAP-TLS、EAP-PEAPを使用する場合は、[EAPメソッド]をクリックします。
EAP-TLSの場合は「スマートカードまたはその他の証明書」が、EAP-PEAPの場合は「保護されたEAP（PEAP）」がそれぞれのリストの最上部に表示されていることを確認し、[OK]をクリックします。
最上部にない場合は、項目を選択して[上へ移動]をクリックしてください。
PEAPの場合、次の追加設定をおこなってください。
  ・「保護されたEAP（PEAP）」を選択し、[編集]をクリック
  ・「セキュリティで保護されたパスワード（EAP-MSCHAPv2）」を選択し、[編集]をクリック
  ・「認証の再試行回数」を「0回」に設定

14 [OK]をクリックし、設定を完了します。

以上でRADIUSサーバーの設定は完了です。

例8:802.1X無線認証を利用する(内蔵RADIUSサーバー機能を利用する場合)

本製品はRADIUSサーバーを用いた無線パソコン認証に対応しています。内蔵RADIUSサーバー機能を使用することにより、RADIUSサーバー(Windows Server等)をお持ちでない環境においても強固なセキュリティーを持つ無線ネットワークを構築することができます。

ここでは例として、内蔵RADIUSサーバー機能を使用したネットワークを構築する方法を説明します。

構成例

条件

・認証には本製品の内蔵RADIUSサーバーを使用し、内部認証にPEAP(MS-PEAP)を使用する。
・接続をおこなうすべてのパソコンにPEAP(MS-PEAP)方式の認証に対応したサプリカントがインストールされ、必要な設定がおこなわれている。
(サプリカントのインストールや設定は、各ソフトウェアのマニュアルをご参照ください。
弊社製無線子機をお使いの場合、添付のクライアントマネージャ3またはクライアントマネージャVのヘルプをご参照ください)

メモ

- **この設定事例ではアクセスポイントが自己発行サーバー証明書を使用するため、P77の図1、図2のようにサプリカント側のサーバー証明書の検証を行わない設定にしてください。Verisign等の発行した証明書を用いて検証を行う場合は別途PKCS#12形式の証明書をインポートする必要があります。**
- **証明書ファイルには、「サーバー証明書(秘密鍵を含む)」、「CA証明書およびRoot証明書までのChainを構成する全ての中間証明書」が含まれている必要があります。**
- **本製品の内蔵RADIUSサーバーは内部認証にTLSを用いた認証にも対応しております。TLS方式で認証を行う場合、クライアント側の証明書に対応したPKCS#12形式の証明書を新たにインポートする必要があります。**

使用機器

対象機器

本製品（WAPM-APG300N/WAPM-AG300N）

必要機器

・クライアントパソコン

設定手順（本製品）

Webブラウザーを使って、本製品の設定画面へログインし、認証の設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[無線設定]－[(802.11aの)無線セキュリティー]をクリックします。

4 以下のように設定して、[設定]をクリックします。

無線の認証	：	WPA/WPA2 mixedmode-EAP
追加認証	：	追加認証を行わない
無線の暗号化	：	TKIP/AES mixed
Key更新間隔	：	60分
ANY接続	：	許可する
プライバシーセパレーター	：	使用しない

無線セキュリティー設定（11a） ? ヘルプ

無線の認証	○認証を行わない ○IEEE802.1x/EAP ○WPA-PSK ○WPA2-PSK ○WPA/WPA2 mixedmode - PSK ○WPA-EAP ○WPA2-EAP ◉WPA/WPA2 mixedmode - EAP
追加認証	◉追加認証を行わない ○MACアドレスリストによる制限 ○MACアドレスリスト+MAC-RADIUS認証 ○MAC-RADIUS認証 認証パスワード ◉MACアドレスを使う ○次のパスワードを使う ○Microsoft NAPを使用する 制限ネットワークに使用するVLAN: 4093
無線の暗号化	○暗号化なし ○WEP(固定値Key) WEP暗号化キー 文字入力・13文字(WEP128) ◉1: ○2: ○3: ○4: ○WEP(自動配信Key) 自動更新Key長 WEP128 WEP（固定値Key）の併用 併用しない 暗号化キー ○TKIP ○AES ◉TKIP/AES mixedmode WPA-PSK(事前共有キー): Key更新間隔: 60 分

［拡張設定］

ANY接続	☑ 許可する
プライバシーセパレーター	使用しない

設定

5 画面左側の[ネットワーク設定]－[RADIUS設定]をクリックします。

6 以下のように設定して、[設定]をクリックします。

内蔵RADIUSサーバー	：	使用する
EAP内部認証	：	PEAP（MS-PEAP）
EAP証明書ファイル形式	：	PKCS#12（*.pfx/*.p12）
EAP証明書ファイル	：	空欄
EAP証明書ファイル・パスワード	：	空欄
Shared Secret	：	abcdefgh（任意の値）
Session-Timeout	：	3600秒
Termination-Action	：	再認証を行う（RADIUS-Request）

内蔵RADIUSサーバー ? ヘルプ

内蔵RADIUSサーバー	☑ 使用する
EAP内部認証	PEAP(MS-PEAP)
EAP証明書ファイル形式	PKCS#12(*.pfx / *.p12)
EAP証明書ファイル	[参照...]
EAP証明書ファイル・パスワード	
Shared Secret	••••••••
Session-Timeout	3600 秒
Termination-Action	◉ 再認証を行う(RADIUS-Request) ○ 再認証を行わない(Default) ○ 送信しない

[設定]

7 以下のように設定して、[新規追加]をクリックします。

サブネット	：	Management（プライマリー）
サーバー	：	内蔵RADIUSサーバーを使用する

8 画面左側の[管理設定]－[ユーザー管理]をクリックします。

9 [登録ユーザーリストの編集]をクリックします。

10 以下のように設定して、[新規追加]をクリックします。

ユーザー名　：　username（任意の値）

ユーザー管理設定 － 登録ユーザーリストの編集　? ヘルプ

編集を終了して前の画面へ戻る

登録ユーザーリストの新規追加　? ヘルプ

ユーザー名

username

新規追加

11 登録ユーザーリストの[修正]をクリックします。

12 以下のように設定して、[修正保存]をクリックします。

パスワード　：ijklmnop(任意の値)

13 画面左側の[無線設定]－[(802.11aの)無線セキュリティー]をクリックします。

14 以下のように設定して、[設定]をクリックします。

無線機能　：使用する
SSID　：値を入力　Shanai(任意の値)

無線基本設定（11a）　? ヘルプ

無線機能	☑使用する
SSID	○ エアステーションのMACアドレスを設定(XXXXXXXXXXXX_A) ◉ 値を入力：Shanai
VLAN ID	1
無線チャンネル	Auto(W52) ※DFSありの場合、気象レーダー等を感知すると自動的にチャンネルが変更されます モード　倍速モード(40MHz) チャンネル変更検出間隔 15 分 ☐子機通信中でもチャンネルを変更する

以上で本製品の設定は完了です。

CLI設定手順

ここまでの設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11a ssid security ssidnum 1 auth
wpa2mixedeap cipher mixed rekey 60
(profile1)man[edit]$ radius internal_server enable eap peap secret
abcdefgh
(profile1)man[edit]$ radius primary enable internal_server
(profile1)man[edit]$ setup authuser add username
(profile1)man[edit]$ setup authuser password username ijklmnop
(profile1)man[edit]$ airset 11a ssid rename ssidnum 1 Shanai
(profile1)man[edit]$ airset 11a wireless enable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

サプリカント側の設定例

図１

クライアントマネージャ３の場合

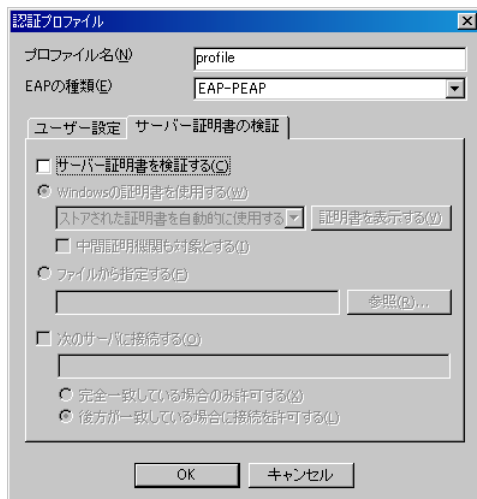



図２

クライアントマネージャVの場合

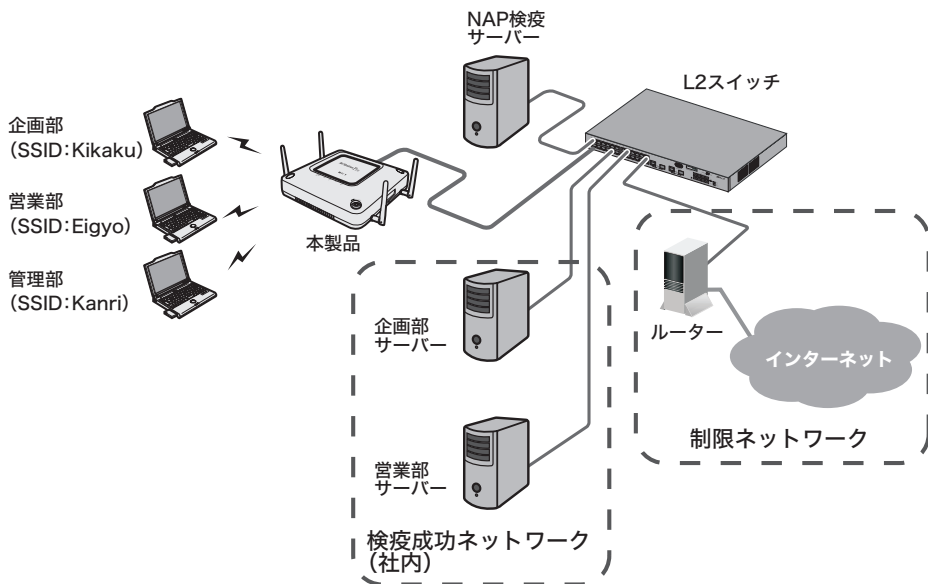
例9:社内ネットワークの安全を自動的に保ちたい(Microsoft NAP)

本製品は、Microsoftネットワークアクセス保護(NAP:Network Access Protection)を用いた無線パソコン認証に対応しており、強固な無線ネットワークと社内ネットワーク等のイントラネットへ接続するクライアントパソコンの正常性ポリシー(※)の管理をおこなうことができます。

※ 正常性ポリシーとは、ファイアウォール、セキュリティーソフトの有無、自動更新などのセキュリティーセンターの設定内容をもとに、パソコンのセキュリティー設定が安全であるかを判断するための基準です。

ここでは例として、ネットワークアクセス保護を利用して本製品を社内ネットワークに導入する方法を説明します。

構成例

条件

・NAP検疫を設定してあるWindows Server 2008が導入されている。
・インターネットに接続できるルーターが導入されている。
・TagVLANに対応したL2スイッチ(例:BS-POE-2124GMR(別売))が導入されている。
・本製品の有線側とL2スイッチがTrunk接続する。
・本製品の管理をおこなう管理部と、本製品の管理VLANを統一する。
・各部署のサーバーにVLAN、SSIDを使用して接続できるようにする。
・各部署のサーバーやパソコンへは通信できないようにする。
・利用者は、Active Directory等で事前登録されている。

使用機器

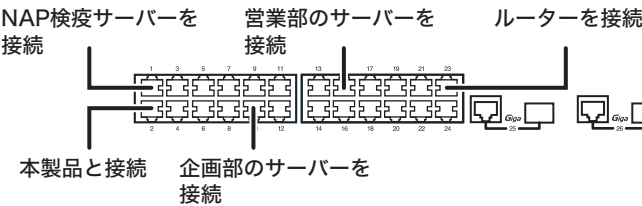
対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・Windows Server 2008(NAP検疫用)
・有線側ネットワーク機器(例:TagVLANに対応したL2スイッチなど)
・クライアントパソコン

設定手順(L2スイッチの設定)

Webブラウザーを使って、ネットワークからL2スイッチへログインし、PoE設定とVLAN設定をおこないます。(ここでは例として、BS-POE2124GMR(別売)を使用します)

1 L2スイッチのマニュアルを参照して、L2スイッチの設定画面を表示します。

2 [基本設定]－[PoE設定]－[PoEポート設定]をクリックします。

3 PoE設定をおこないます。
以下のようにポート2を設定して、[設定]をクリックします。

優先度　　　：高
ハイパワー　：afhigh-power
(他の項目は、初期値のまま使用します)

PoEポート設定

ポート	PoE有効化	優先度	ハイパワー
1	ON	低	Disable
2	ON	高	af high-power
3	ON	低	Disable af high-power
4	ON	低	Disable
5	ON	低	Disable
6	ON	低	Disable
7	ON	低	Disable

4 [詳細設定]－[VLAN設定]－[VLANステータス]をクリックします。

5 企画部のVLAN(101)を作成します。
以下のように項目を設定して、[設定]をクリックします。

VLAN ID ： 101
VLAN名 ： Kikaku
VLAN Management ： チェックなし
ポート ： 2を「Static Tagged」、3～12を「Static Untagged」、1、13～26を「Not Member」

6 営業部のVLAN(102)を作成します。以下のように項目を設定して、[設定]をクリックします。

VLAN ID　：102
VLAN名　：Eigyo
VLAN Management：チェックなし
ポート　：2を「Static Tagged」、13～22を「Static Untagged」、1、3～12、23～26を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
101	–	T	U	U	U	U	U	U	U	U	U	U	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Kikaku
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged　U:Static Untagged　–:Not Member

新規VLAN 作成

VLAN ID:	102 (1–4094)
VLAN 名:	Eigyo
VLAN Management:	☐

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	○	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	○	○	○	○	○	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	○	○	○	○
Not Member	◉	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	○	○	○	○	○	○	○	○	○	○	◉	◉	◉	◉

[設定] [再読込] [クリア]

7 NAP修復用のVLAN(1000)を作成します。以下のように項目を設定して、[設定]をクリックします。

VLAN ID　　　　　　：1000
VLAN名　　　　　　：NAPrepair
VLAN Management：チェックなし
ポート　　　　　　：2を「Static Tagged」、23を「Static Untagged」、1、3〜22、24〜26を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
101	–	T	U	U	U	U	U	U	U	U	U	U	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Kikaku
102	–	T	–	–	–	–	–	–	–	–	–	–	U	U	U	U	U	U	U	U	U	U	–	–	–	–	Eigyo
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged　U:Static Untagged　–:Not Member

新規VLAN 作成

VLAN ID:	1000 (1–4094)
VLAN 名:	NAPrepair
VLAN Management:	☐

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	○	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◉	○	○	○
Not Member	◉	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	○	◉	◉	◉

[設定] [再読込] [クリア]

8 VLANステータスに表示されているVLAN 1の欄にある[編集]をクリックします。

9 管理部のVLAN(1)を作成します。
以下のように設定を変更して、[設定]をクリックします。

VLAN ID　　　　　　： 1
VLAN名　　　　　　： Kanri
VLAN Management： チェックあり
ポート　　　　　　： 2を「Static Tagged」、1、3〜22、24〜26を「Static Untagged」、23を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
101	−	T	U	U	U	U	U	U	U	U	U	U	−	−	−	−	−	−	−	−	−	−	−	−	−	−	Kikaku
102	−	T	−	−	−	−	−	−	−	−	−	−	U	U	U	U	U	U	U	U	U	U	−	−	−	−	Eigyo
1000	−	T	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	U	−	−	−	NAPrepair
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged　U:Static Untagged　−:Not Member

新規VLAN 作成

VLAN ID:	1 (1−4094)
VLAN 名:	Kanri
VLAN Management:	☑

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	○	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	◉	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	○	◉	◉	◉
Not Member	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◉	○	○	○

[設定] [再読込] [クリア]

10 [詳細設定]−[VLAN設定]−[VLANポート設定]をクリックします。

11 各ポートにPVIDを設定します。
以下のように項目を設定して、[設定]をクリックします。

ポート1、2、24〜26　： 1
ポート3〜12　　　　： 101
ポート13〜22　　　 ： 102
ポート23　　　　　 ： 1000

VLANポート設定

ポート	1	3	5	7	9	11	13	15	17	19	21	23	25
PVID	1	101	101	101	101	101	102	102	102	102	102	1000	1
ポート	2	4	6	8	10	12	14	16	18	20	22	24	26
PVID	1	101	101	101	101	101	102	102	102	102	102	1	1

[設定] [再読込]

以上でL2スイッチの設定は完了です。
続いて、Windows Server 2008の設定をおこないます。

設定手順(Windows Server 2008の設定)

Windows Server 2008を使用してNAP(Network Access Protection)機能を実現する方法を提供するため、Windows Server 2008(以下サーバー)において以下の役割が構成されていることを確認してください。構成されていない場合は、追加インストールをおこなってください。
(設定に関しては、「サーバーマネージャ」を使用して説明します)

サーバーマネージャ役割

1. Active Directory(ドメインサービス)
   以下を参照してください。

2. Active Directory(証明書サービス)
   エンタープライズのルートCAとして構成します。

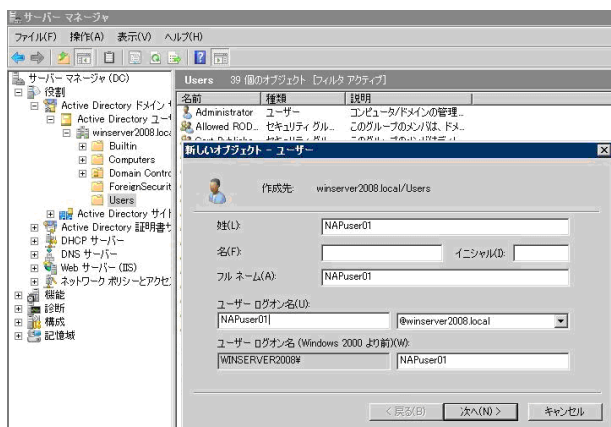
3. DNSサーバー
   プライマリーDNSとして構成します。

4. ネットワークポリシーとアクセスサービス(NPS)
   「NPS(シナリオウィザードを使用したNAPの構成)」(P86)を参照してください。

Active Directory(ドメインサービス設定)

1 **[スタート]－[管理ツール]－[サーバーマネージャ]を選択します。**

2 **「サーバーマネージャ」が起動したら、[役割]－[Active Directoryドメインサービス]－[Active Directoryユーザーとコンピューター]－[サーバー名(任意)]－[Users]を開きます。**

3 [Users]内で右クリックし、ユーザー(例:NAPuser01)をウィザードの指示にしたがって追加します。

※Windows Server 2008では、「パスワードは複雑さの要件を満たす必要がある」ポリシーが初期設定で有効となっているため、簡単なパスワードは設定できません。パスワード設定時は、複雑なパスワードを設定するか、グループポリシーを変更してパスワードを設定してください。

RADIUSクライアント

1 「サーバーマネージャー」画面より、[役割]－[ネットワークポリシーとアクセスサービス]－[NPS(ローカル)]－[RADIUSクライアントとサーバー]－[RADIUSクライアント]を右クリックして[新規RADIUSクライアント]を選択します。

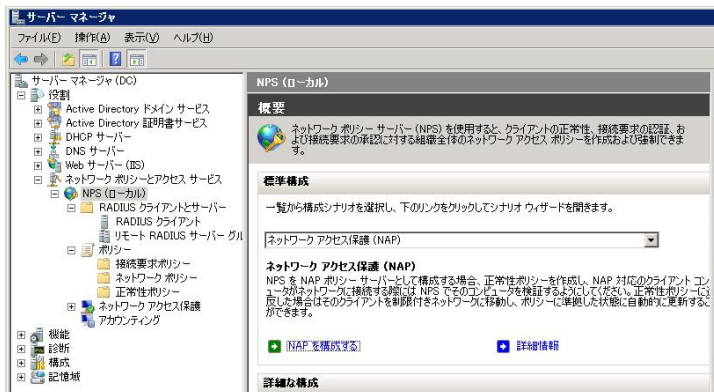
2 以下のよう設定して、[OK]をクリックします。

フレンドリ名	：	WAPM-APG300N
アドレス（IPまたはDNS）	：	test_napserver.local
ベンダ名	：	RADIUS Standard
共有シークレット	：	nappassword（手動）
追加オプション	：	「RADIUSクライアントがNAPに対応している」が有効

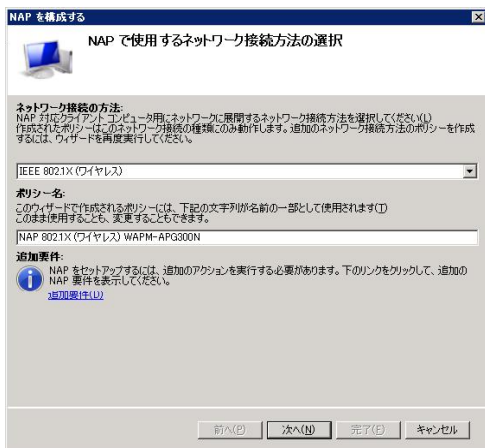
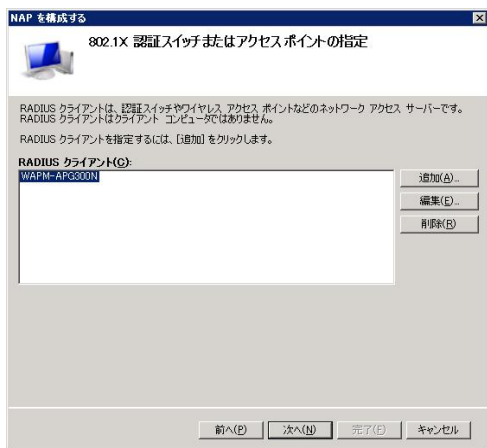
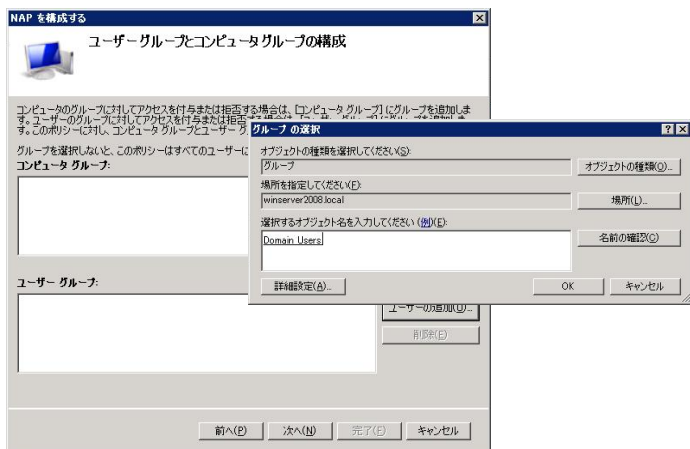
※「共有シークレット」は、本製品の「RADIUS設定」にある「Shared Secret」と同じ値を設定する必要があります。

NPS（シナリオウィザードを使用したNAPの構成）

1 「サーバーマネージャー」画面より、[役割]－[ネットワークポリシーとアクセスサービス]－[NPS（ローカル）]をクリックします。

2 「標準構成」で、「ネットワークアクセス保護(NAP)」を選択して[NAPを構成する]をクリックします。

※ [NAPを構成する]をクリックすると、ウィザード画面が表示されます。

3 以下の内容を設定して、[次へ]をクリックします。

ネットワーク接続の方法	:	IEEE802.1X(ワイヤレス)
アドレス(IPまたはDNS)	:	test_napserver.local
ベンダ名	:	RADIUS Standard
共有シークレット	:	nappassword(手動)
ポリシー名	:	任意のポリシー名 (例:NAP802.1X(ワイヤレス)WAPM-APG300N)

4 「RADIUSクライアント」の手順２（P86）で追加したRADIUSクライアント（WAPM-APG300N）を選択して、[次へ]をクリックします。

5 「Active Directory（ドメインサービス設定）」の手順３（P85）で作成したユーザーグループを指定して、[次へ]をクリックします。

※ 使用する環境に合わせてグループを追加し、グループごとに設定を分けることもできます。

6 EAPの種類を設定して、[次へ]をクリックします。

EAPの種類　：セキュリティーで保護されたパスワード（PEAP-MS-CHAP）が有効

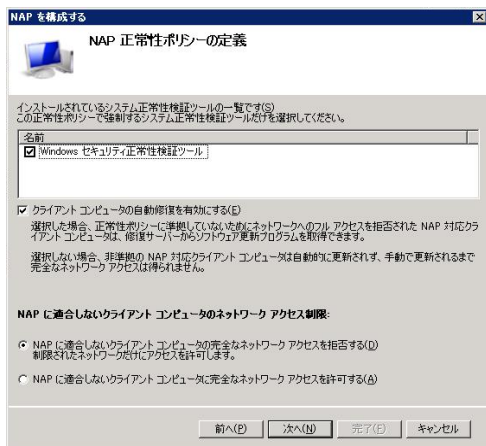
※NPSサーバー証明書は、事前に追加したものが表示されます。

7 設定を変更せずに、そのまま[次へ]をクリックします。

※ 上記は、NAP検疫後に接続する組織ネットワークのVLANと制限されたネットワークのVLANを設定する画面です。本設定事例では、上記の内容は設定しません。

8 NAP正常性ポリシーを設定して、[次へ]をクリックします。

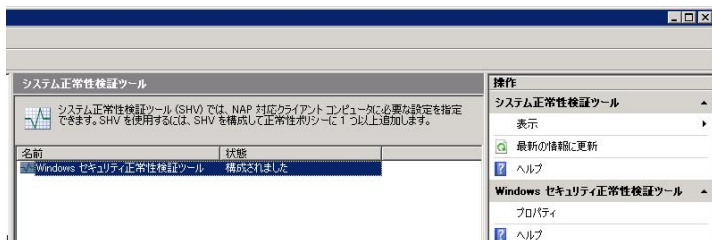
システム正常性検証ツール ： Windowsセキュリティー正常性検証ツール
（「クライアントコンピュータの自動修復を有効にする」が有効）

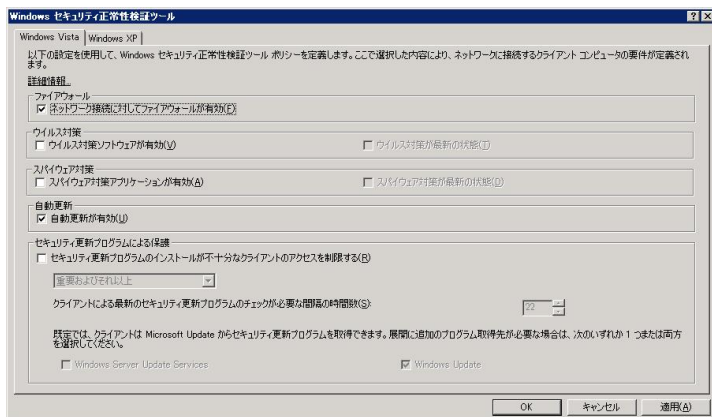
NAPに適合しないクライアントコンピューターのネットワークアクセス制限
： NAPに適合しないクライアントコンピュータの完全なネットワークアクセスを拒否する

※「システム正常性検証ツール」が複数インストールされている場合は、使用するものだけにチェックマークを付けてください。

9 設定内容を確認し、[完了]をクリックします。

システム正常性検証ツール

1 「サーバーマネージャー」画面より、[役割]－[ネットワークポリシーとアクセスサービス]－[NPS(ローカル)]－[ネットワークアクセス保護]－[システム正常性検証ツール]をクリックします。

2 画面右側の「Windowsセキュリティ正常性検証ツール」からプロパティ画面を表示させます。

3 「Windowsセキュリティ正常性検証ツールのプロパティ」画面が表示されたら、[構成]をクリックします。

4 Windows Vista/XPのポリシーにて、「ファイアウォール」と「自動更新」にのみチェックマークを付けて、[OK]をクリックします。

※ 上記は、接続クライアントに対する検疫のポリシーを設定する画面です。本設定事例では、「ファイアウォール」と「自動更新」以外の内容は設定しません。

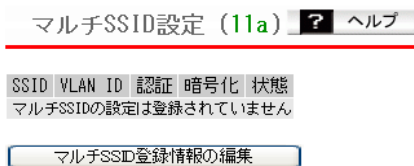
以上でWindows Server 2008の設定は完了です。

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、VLANおよびマルチSSIDの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[無線設定]-[(802.11aの)マルチSSID]をクリックし、[マルチSSID登録情報の編集]をクリックします。

4 企画部のネットワークの設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

SSID	：	Kikaku
VLANID	：	101
無線の認証	：	IEEE802.1x/EAP
追加認証	：	Microsoft NAPを使用する （制限ネットワークに使用するVLAN　1000）
無線の暗号化	：	WEP（自動配信Key） （自動更新Key長　WEP128）
ANY接続	：	許可する（チェックあり）
プライバシーセパレーター	：	SSIDセパレーター

5 [設定]をクリックします。

6 同様に、営業部のネットワークの設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

SSID　：　Eigyo
VLANID　：　102
無線の認証　：　IEEE802.1x/EAP
追加認証　：　Microsoft NAPを使用する
（制限ネットワークに使用するVLAN　1000）
無線の暗号化　：　WEP（自動配信Key）
（自動更新Key長　WEP128）
ANY接続　：　許可する（チェックあり）
プライバシーセパレーター　：　SSIDセパレーター

7 [設定]をクリックします。

8 画面左側の[無線設定]－[(802.11aの)無線セキュリティー]をクリックします。

9 管理部の無線セキュリティー設定をおこないます。以下のように項目を設定して、[新規追加]をクリックします。

無線の認証 ： IEEE802.1x/EAP
追加認証 ： Microsoft NAPを使用する
（制限ネットワークに使用するVLAN　1000）
無線の暗号化 ： WEP（自動配信Key）
（自動更新Key長　WEP128）
ANY接続 ： 許可する（チェックあり）
プライバシーセパレーター ： 使用しない

無線セキュリティー設定（11a）
ヘルプ

無線の認証
認証を行わない
IEEE802.1x/EAP
WPA-PSK
WPA2-PSK
WPA/WPA2 mixedmode - PSK
WPA-EAP
WPA2-EAP
WPA/WPA2 mixedmode - EAP

追加認証
追加認証を行わない
MACアドレスリストによる制限
MACアドレスリスト+MAC-RADIUS認証
MAC-RADIUS認証
認証パスワード
MACアドレスを使う
次のパスワードを使う
Microsoft NAPを使用する
制限ネットワークに使用するVLAN: 1000

無線の暗号化
暗号化なし
WEP(固定値Key)
WEP暗号化キー 文字入力・13文字(WEP128)
1:
2:
3:
4:
WEP(自動配信Key)
自動更新Key長 WEP128
WEP（固定値Key）の併用 併用しない
暗号化キー
TKIP
AES
TKIP/AES mixedmode
WPA-PSK(事前共有キー):
●●●●●●●●●●●●●
Key更新間隔: 60 分

[拡張設定]
ANY接続 許可する
プライバシーセパレーター 使用しない

設定

10 [設定]をクリックします。

11 画面左側の[無線設定]－[（802.11aの）無線基本]をクリックします。

12 管理部の無線基本設定をおこないます。以下のように項目を設定して、[設定]をクリックします。

無線機能　：使用する
SSID　：値を入力する(Kanri)
VLAN ID　：1
(上記以外の設定値は、初期値のまま使用します)

無線基本設定 (11a)　? ヘルプ

無線機能	☑使用する
SSID	○ エアステーションのMACアドレスを設定(XXXXXXXXXXXX_A) ◉ 値を入力：Kanri
VLAN ID	1
無線チャンネル	Auto(W52)　(現在のチャンネル：36+40) ※DFSありの場合、気象レーダー等を感知すると自動的にチャンネルが変更されます モード　倍速モード(40MHz)

13 [設定]をクリックします。

14 画面左側の[ネットワーク設定]－[RADIUS設定]をクリックします。

15 プライマリーサーバーを以下のように項目を設定して、[新規追加]をクリックします。

プライマリーサーバー　：使用する
サーバー名　：RADIUSサーバーのIPアドレスまたはDNS解決可能なドメイン名
Shared Secret　：RADIUSサーバーと同じShared Secret
(上記以外の設定値は、初期値のまま使用します)

RADIUS設定　? ヘルプ

RADIUS設定の新規追加　? ヘルプ

サブネット	Management(プライマリー)
サーバー名	PrimaryServer
認証ポート	1812
Accounting	☑ 使用する
Accountingポート	1813
Shared Secret	••••••••
Session-Timeout	3600 秒
Termination-Action	☐ Termination-Action 属性を使用する

新規追加

16 同様にセカンダリーサーバーを以下のように項目を設定して、[新規追加]をクリックします。

セカンダリーサーバー	：	使用する
サーバー名	：	RADIUSサーバーのIPアドレスまたはDNS解決可能なドメイン名
Shared Secret	：	RADIUSサーバーと同じShared Secret

（上記以外の設定値は、初期値のまま使用します）

RADIUS設定 ? ヘルプ

RADIUS設定の新規追加 ? ヘルプ

サブネット	Management(セカンダリー)
サーバー名	SecondaryServer
認証ポート	1812
Accounting	☑ 使用する
Accountingポート	1813
Shared Secret	●●●●●●●●●
Session-Timeout	3600 秒
Termination-Action	☐ Termination-Action 属性を使用する

新規追加

17 画面左側の[LAN設定]－[サブネット設定]をクリックします。[サブネットの編集]をクリックします。

18 「サブネットの表示/操作」に登録されている「Management」欄の[編集]をクリックします。

19 管理用サブネット(Management)を以下のように設定して、[修正保存]をクリックします。

サブネット名	:	Management
サブネット種別	:	管理サブネット
VLAN ID	:	1
IPアドレスの取得方法	:	手動設定
IPアドレス	:	192.168.11.100(255.255.255.0) (RADIUSクライアントとして登録したIPアドレス)
ルーティング	:	ルーティング
デフォルトゲートウェイ	:	空欄
DNS	:	空欄
動的経路	:	受信「RIPv1」と「RIPv2」にのみチェックマークを付ける
UPnP IGD	:	使用しない
MTU	:	1500
DHCPサーバー	:	使用しない

サブネット情報の編集　? ヘルプ

編集を終了して前の画面へ戻る

サブネット情報の編集　? ヘルプ

サブネット名	Management
サブネット種別	◉管理サブネット
VLAN ID	1
IP アドレスの取得方法	◉ 手動設定 ○ DHCP クライアント
IP アドレス	IP アドレス 192.168.11.100 サブネットマスク 255.255.255.0
ルーティング	ルーティング
デフォルトゲートウェイ	手動設定
DNS	プライマリーサーバー: セカンダリーサーバー:
動的経路	送信：☐RIPv1 ☐RIPv2 受信：☑RIPv1 ☑RIPv2
UPnP IGD	使用しない
MTU	1500
DHCP サーバー	◉使用しない ○サブネットにDHCPサーバー機能を提供する ○サブネットにDHCPサーバー機能をRelayする

修正保存

20 [設定]をクリックします。

21 画面左側の[LAN設定]－[LANポート]をクリックします。

22 以下のように設定して、[設定]をクリックします。

VLAN モード　　　　　：Tagged Port

23 [設定]をクリックします。

以上で本製品の設定は完了です。
続いて無線パソコンからそれぞれのSSIDを使ってネットワークに接続します。

クライアントの設定手順

NAP検疫をおこなうためにクライアント側の設定をします。Windowsドメイン参加を使用する場合、Windows端末はグループポリシーに従って自動的にNAPクライアントの設定が反映されます。ここではドメイン参加をおこなわずに、手動設定にてNAPクライアントの設定をする方法を案内します。

※ NAP検疫に対応しているクライアント側のOSは、Windows Vista/XP(SP3以降)となります。

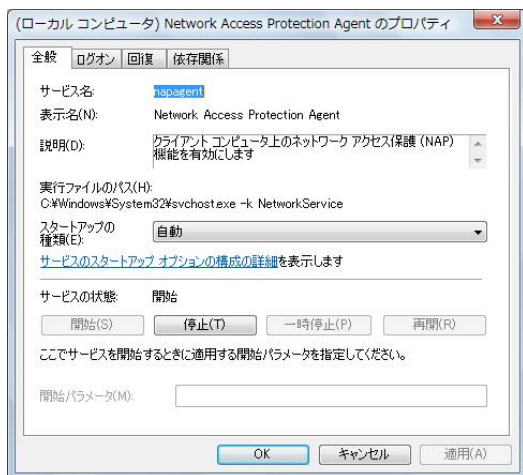
Windows Vistaの設定

クライアント側のOSがWindows Vistaの場合は、以下の手順で設定してください。

1 [スタート]－[アクセサリ]－[ファイル名を指定して実行]を選択します。

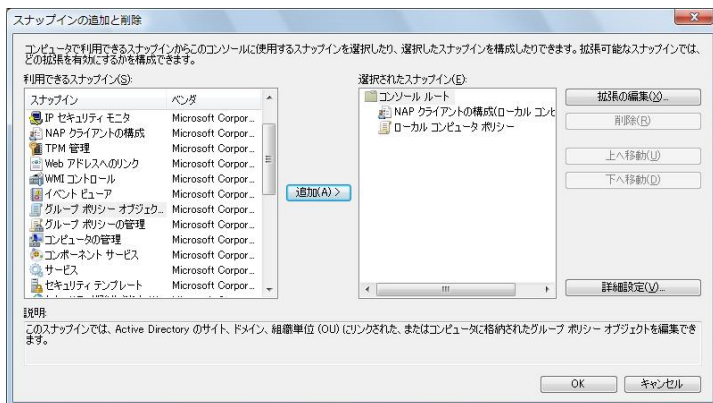
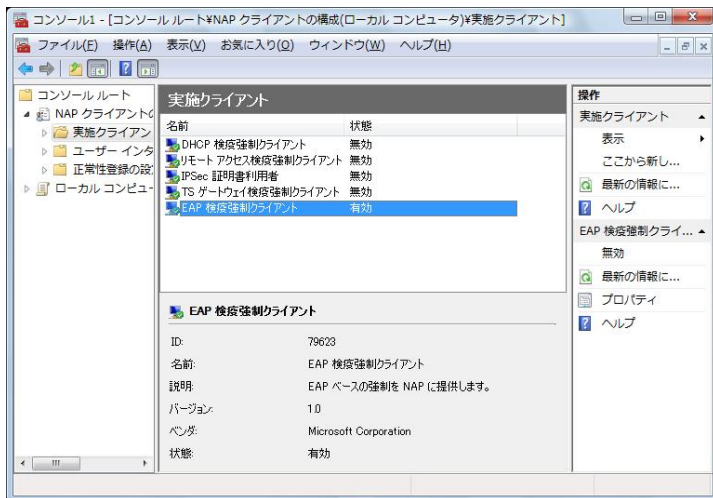
2 名前欄に「services.msc」と入力して、[OK]をクリックします。

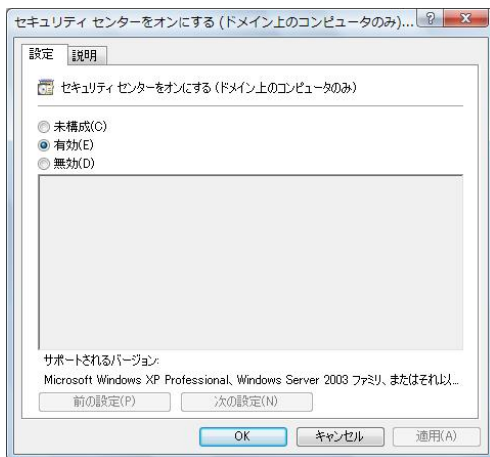
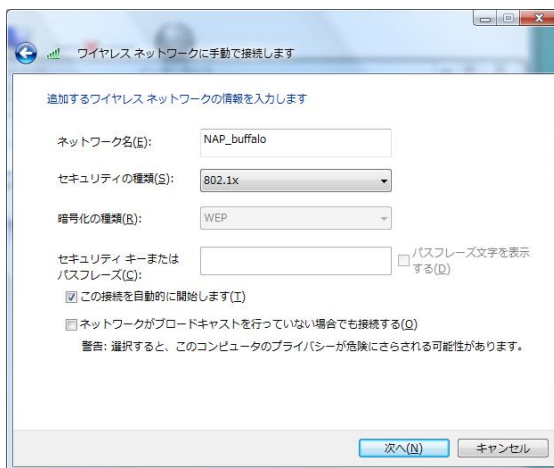
3 サービス一覧から「Network Access Protection Agent」を右クリックし、[プロパティ]を選択します。

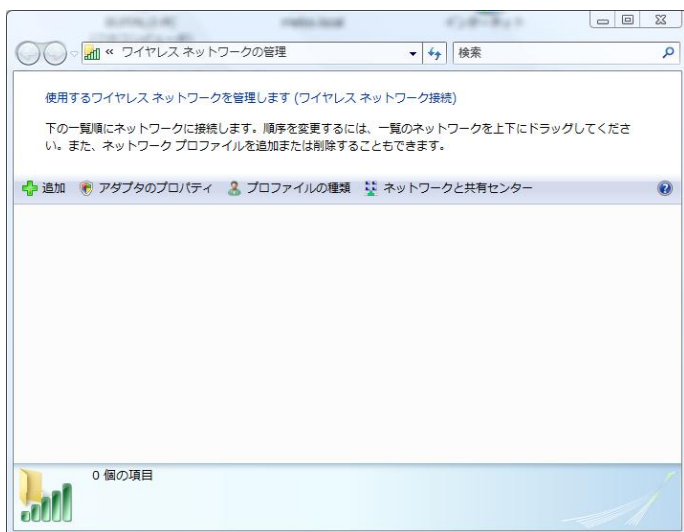
4 スタートアップの種類を「自動」に設定し、サービスの状態欄にある[開始]をクリックして、[OK]をクリックします。

5 [スタート]－[アクセサリ]－[ファイル名を指定して実行]を選択します。

6 名前欄に「mmc」と入力して、[OK]をクリックします。

7 コンソール1画面が表示されたら、「ファイル」－「スナップインの追加と削除」を選択します。

8 スナップインの追加と削除画面にて、「NAPクライアントの構成」と「グループポリシーオブジェクトエディタ」を追加し、[OK]をクリックします。

9 コンソール1の左画面にて、「コンソールルート」－「NAPクライアントの構成」－「実施クライアント」を選択し、右画面の「EAP検疫強制クライアント」を右クリックして、「有効」に設定します。

10 コンソール1の左画面にて、「コンソールルート」－「ローカルコンピュータポリシー」－「管理テンプレート」－「Windowsコンポーネント」－「セキュリティセンター」を選択し、右画面の「セキュリティセンターをオンにする(ドメイン上のコンピュータのみ)」を右クリックして、[プロパティ]を選択します。

11 「有効」を選択して[OK]をクリックします。

12 コントロールパネル内の「ネットワーク共有センター」をダブルクリックし、「ワイヤレスネットワークの管理」をクリックします。

13 「追加」をクリックして、「ネットワークプロファイルを手動で作成します」を選択します。

14 以下の設定をおこなって、[次へ]をクリックします。

ネットワーク名　　　：本製品に設定されているSSIDと同じ設定にします。
セキュリティの種類 ：本製品に設定されているセキュリティと同じ設定にします。
暗号化の種類　　　：本製品に設定されている暗号化の種類と同じ設定にします。

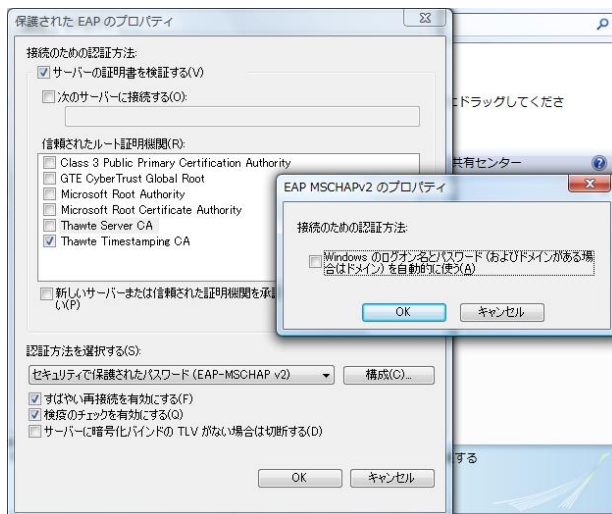
15 「接続の設定を変更します」をクリックします。

16 「セキュリティ」タブをクリックして、「ネットワークの認証方式の選択」で「Microsoft:保護されたEAP(PEAP)」を選択し、[設定]をクリックします。

17 「サーバーの証明書を検証する」にチェックマークが付いていることを確認して「信頼されたルート証明書機関」にて使用するサーバーを選択します。

18 「認証方式を選択する」で「セキュリティで保護されたパスワード(EAP-MSCHAP v2)」を選択します。

19 「すばやい再接続を有効にする」と「検疫のチェックを有効にする」にチェックマークを付け、[構成]をクリックします。

20 EAP MSCHAP v2のプロパティ画面にて、「Windowsのログオン名とパスワード(およびドメインがある場合はドメイン)を自動的に使う」のチェックマークを外します。

以上でWindows Vistaの設定は完了です。

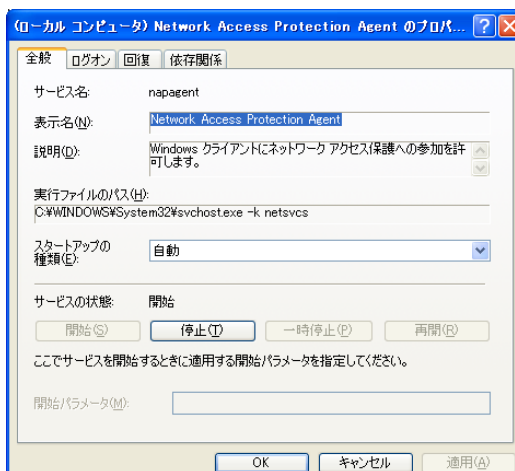
Windows XPの設定

クライアント側のOSがWindows XPの場合は、以下の手順で設定してください。

1 [スタート]ー[ファイル名を指定して実行]を選択します。

2 名前欄に「services.msc」と入力して、[OK]をクリックします。

3 サービス一覧から「Network Access Protection Agent」を右クリックし、[プロパティ]を選択します。

4 スタートアップの種類を「自動」に設定し、サービスの状態欄にある[開始]をクリックして、[OK]をクリックします。

5 [スタート]−[ファイル名を指定して実行]を選択します。

6 名前欄に「mmc」と入力して、[OK]をクリックします。

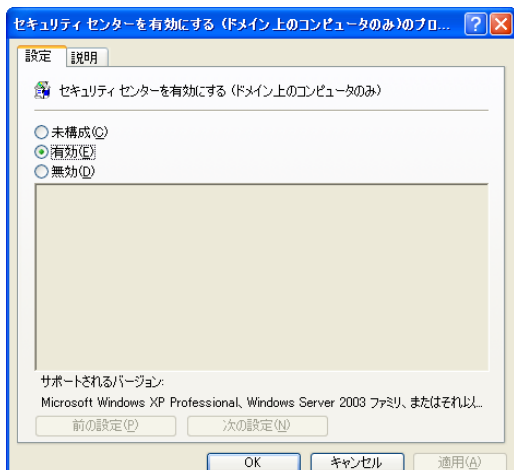
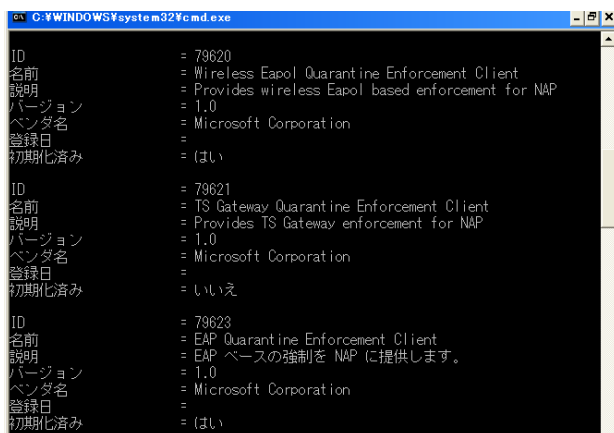
7 コンソール1画面が表示されたら、「ファイル」−「スナップインの追加と削除」を選択します。

8 [追加]をクリックします。

9 「スタンドアロンスナップインの追加」画面が表示されたら、「グループポリシー」を選択し、[追加]をクリックします。

10 グループポリシーオブジェクトの選択画面が表示されたら、[完了]をクリックします。

11 コンソール1の左画面にて、「コンソールルート」−「ローカルコンピュータポリシー」−「コンピュータの構成」−「管理用テンプレート」−「Windowsコンポーネント」−「セキュリティセンター」を選択し、右画面の「セキュリティセンターを有効にする(ドメイン上のコンピュータのみ)」を右クリックして、[プロパティ]を選択します。

12 「有効」を選択して、[OK]をクリックします。

13 [スタート]－[(すべての)プログラム]－[アクセサリ]－[コマンドプロンプト]を選択します。

14 EAP検疫強制クライアントを起動する「EAP Quarantine Enforcement Client」コマンドを実行します。

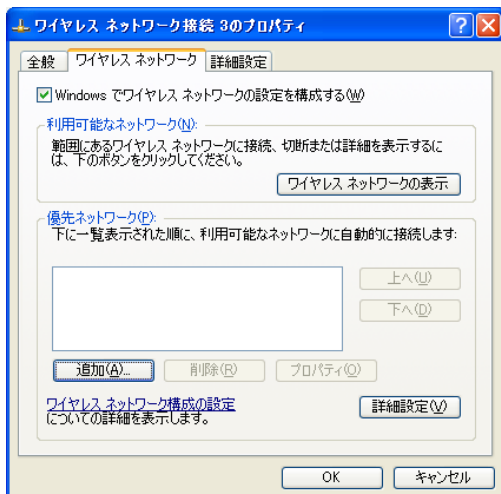
「netsh nap client set enforcement ID=79620 ADMIN=“ENABLE”　と入力し、[Enter]キーを押します。

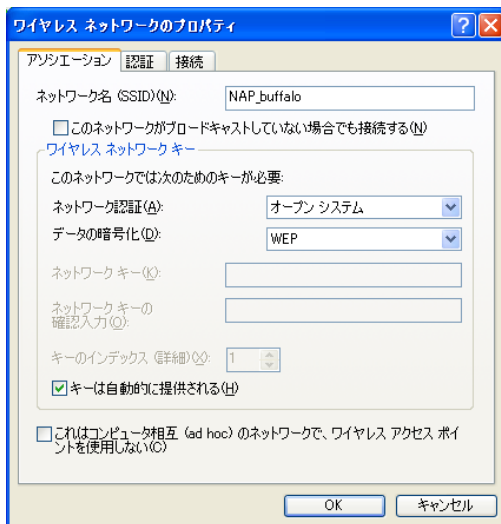
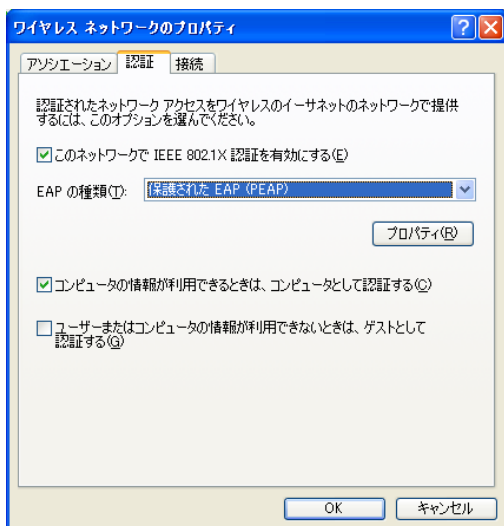
コマンドが実行されているかを確認するためには、「netsh nap client show state」と入力し、[Enter]キーを押してください。

表示された「実施クライアントの状態」の中で、ENABLE設定したEAP Quarantine Enforcement Clientが「初期化済み=はい」となっていることを確認してください。

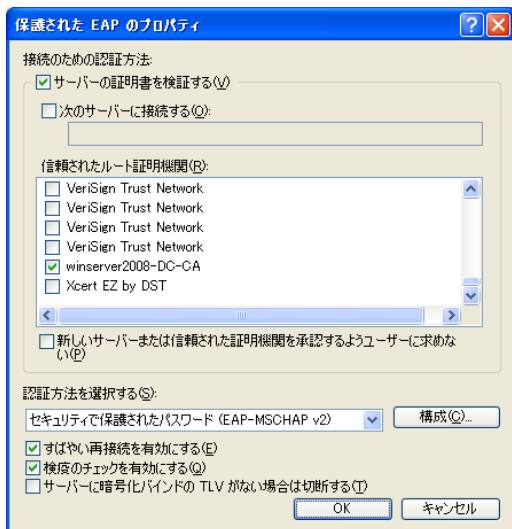
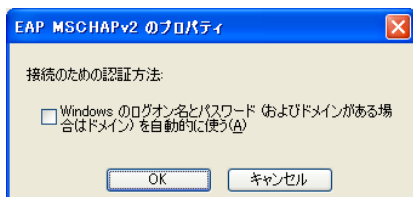
15 [スタート]-[接続]を右クリックして、[開く]を選択します。

16 無線接続するデバイスを右クリックして、[プロパティ]を選択します。

17 「ワイヤレスネットワーク」タブをクリックし、[追加]をクリックします。

18 「アソシエーション」タブにて以下の設定をします。

ネットワーク名(SSID) ： 本製品に設定されているSSID
ネットワーク認証 ： 本製品と同じ種類のセキュリティを設定します。
データの暗号化 ： 本製品と同じ暗号化を設定します。

19 「認証」タブをクリックして、「EAPの種類」で「保護されたEAP(PEAP)」を選択し、[プロパティ]をクリックします。

20 「サーバーの証明書を検証する」にチェックマークが付いていることを確認して「信頼されたルート証明書機関」にて使用するサーバーを選択します。

21 「認証方式を選択する」で「セキュリティで保護されたパスワード(EAP-MSCHAP v2)」を選択します。

22 「すばやい再接続を有効にする」と「検疫のチェックを有効にする」にチェックマークを付け、[構成]をクリックします。

23 EAP MSCHAP v2のプロパティ画面にて、「Windowsのログオン名とパスワード(およびドメインがある場合はドメイン)を自動的に使う」のチェックマークを外します。

以上でWindows XPの設定は完了です。

CL設定手順

ここまでの本製品の設定をCLI を使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$ airset 11a ssid add ssidname Kikaku vlanid 101
auth eap cipher wep rekey 60 key 128
(profile1)man[edit]$ airset 11a ssid addsecurity ssidname Kikaku
mode nap bgvlan 1000
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Kikaku enable
(profile1)man[edit]$ airset 11a ssid privacy ssidname Kikaku ssid
(profile1)man[edit]$ airset 11a ssid add ssidname Eigyo vlanid 102
auth eap cipher wep rekey 60 key 128
(profile1)man[edit]$ airset 11a ssid addsecurity ssidname Eigyo mode
nap bgvlan 1000
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Eigyo enable
(profile1)man[edit]$ airset 11a ssid privacy ssidname Eigyo ssid
(profile1)man[edit]$ airset 11a ssid rename ssidnum 1 Kanri
(profile1)man[edit]$ airset 11a ssid vlan ssidname Kanri vlanid 1
(profile1)man[edit]$ airset 11a ssid security ssidname Kanri auth
eap cipher wep rekey 60 key 128
(profile1)man[edit]$ airset 11a ssid addsecurity ssidname Kanri mode
nap bgvlan 1000
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Kanri enable
(profile1)man[edit]$ airset 11a ssid privacy ssidname Kanri ssid
(profile1)man[edit]$ airset 11a wireless enable
(profile1)man[edit]$ radius primary enable server [RADIUSプライマリー
サーバー名] secret [SharedSecret]
(profile1)man[edit]$ radius secondary enable server [RADIUSセカンダ
リーサーバー名] secret [SharedSecret]
(profile1)man[edit]$ ip lan address 192.168.11.100/24 force
(profile1)man[edit]$ ether port 1 vlan mode tagged
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

例10:スパニングツリーを利用する

スパニングツリーは、本製品や一部のネットワーク機器に搭載されている機能です。
ここでは、スパニングツリーを利用したネットワークの構成例を説明します。

スパニングツリーについて

利用用途

スパニングツリーに対応した機器(弊社製インテリジェントスイッチなど)と組み合わせることで、自動的にループ回避と冗長性を持ったネットワーク構成が可能になります。

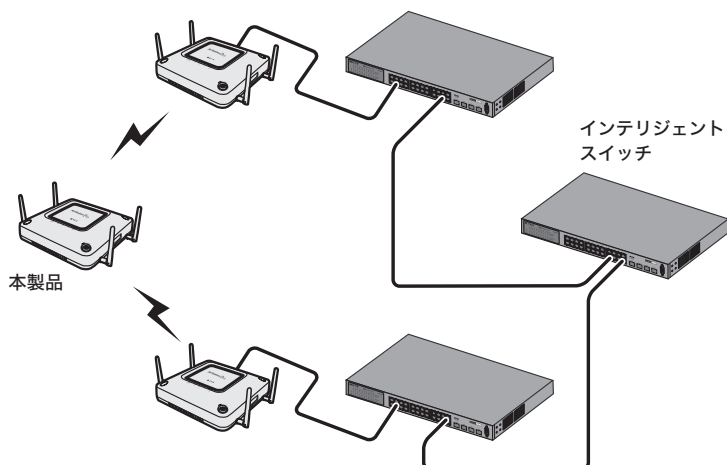
おもな利点

・LANにおけるループ構成を自動で回避できます
(ブロードキャストストームを回避したり、MACテーブルの学習が正常におこなえるように監視します)
・ネットワーク構成に冗長性を持たせることができます
(重要なパスが途切れた際にも代理として予備のリンクを検出しループを防ぎながら接続することができます)

スパニングツリーの種類(Legacy/Rapid)

Legacy(IEEE802.1D) : BPDUパケットを利用して、他のブリッジとスパニングツリープロトコルによるポート接続情報のやりとりをおこなうことで、ループの検出や回避、冗長構成などを実現するための制御方法です。構成内容によっては、収束するまでに時間がかかります。(最大で50秒間の通信断が発生してしまいます)

Rapid(IEEE802.1w) : Legacyのスパニングツリーをより高速化させたプロトコルです。ただし、構成する機器がRapidスパニングツリーに対応していない場合は、Legacyとして扱われます。

構成例

条件

・すでにスパニングツリー機能を持ったネットワーク機器が設置､運用されている。
・本製品同士はリピーター機能(WDS)で接続する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・スパニングツリー機能に対応したインテリジェントスイッチ(例:BS-G2024MR(別売)など)
・クライアントパソコン

設定手順(本製品)

Webブラウザーを使って､本製品の設定画面へログインし､スパニングツリーの設定をおこないます。

1 別冊の｢ユーザーズマニュアル｣を参照して､本製品の設定画面を表示します。

2 ｢詳細設定｣をクリックします。

3 画面左側の[ネットワーク設定]－[ブリッジ]をクリックします。以下のように項目を設定して、[設定]をクリックします。

Aging Time ： 300
スパニングツリー ： 使用する（チェックあり）
モード ： RapidSTP
その他のパラメーター ： 初期設定のまま変更なし

※お使いの環境によっては、Hello TimeやMax Ageなど、パラメーターを個別に設定する必要があります。

4 画面左側の[無線設定]－[（使用する無線規格の）無線基本]をクリックします。「無線チャンネル」を「Auto」以外の固定のチャンネルに変更して、[設定]をクリックします。

※リピーター機能（WDS）を使用するには、通信するエアステーションの無線チャンネルをすべて同じ設定にする必要があります。

5 画面左側の[無線設定]－[(使用する無線規格の)リピーター機能]をクリックします。
「リピーター機能(WDS)」を「使用する」に変更して、[設定]をクリックします。

6 [通信可能なアクセスポイントの編集]をクリックします。

7 下記のように変更して、[新規追加]をクリックします。

アクセスポイントの無線側MACアドレス:アクセスポイントの無線側MACアドレス
VLANモード　:　Untagged Port
無線の暗号化　:　AES
WEP/PSK　:　9876543210(任意の値)

リピーター機能(WDS)設定 － 通信可能なアクセスポイントの編集 (11g) ヘルプ

編集を終了して前の画面へ戻る

通信可能なアクセスポイントの新規追加 ヘルプ

アクセスポイントの無線側MACアドレス	XX:XX:XX:XX:XX:XX
VLAN モード	Untagged Port　VLAN ID 1
暗号化	AES
WEP/PSK	••••••••••

本機の無線側MACアドレス[XX:XX:XX:XX:XX:XX]

新規追加

通信可能なアクセスポイント ヘルプ

MACアドレス	暗号化	VLAN ID	状態	操作
通信可能なアクセスポイントが登録されていません				

8 通信相手側のエアステーションで、手順1～7までの手順をおこないます。

以上で本製品の設定は完了です。
設定が完了すると、Rapidスパニングツリープロトコルが動作し、ループ回避と冗長性を持ったネットワーク構成が自動的に設定されます。

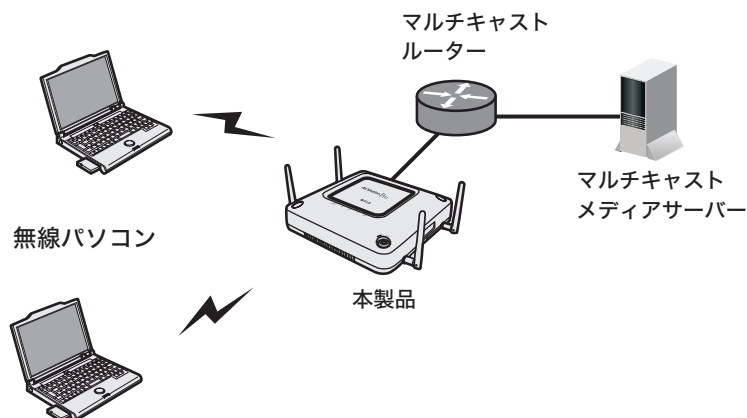
CL設定手順

本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$ bridge aging 300
(profile1)man[edit]$ bridge stp mode rstp
(profile1)man[edit]$ bridge stp enable
(profile1)man[edit]$ airset 11g channel 1 bandwith 20m
(profile1)man[edit]$ airset 11g wds enable
(profile1)man[edit]$ airset 11g wds add XX:XX:XX:XX:XX:XX
(profile1)man[edit]$ airset 11g wds security XX:XX:XX:XX:XX:XX
wpapsk cipher aes key 9876543210
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

例11：マルチキャストスヌーピングを利用する

本製品は、マルチキャストスヌーピング機能に対応しています。この機能を使用することで、マルチキャスト管理パケットの監視をおこない、不要なIPマルチキャストパケットのフラッディングを抑制することができるようになります。
ここでは例として、マルチキャストスヌーピング機能を使用したネットワーク設定について説明します。

構成例

条件

・すでにネットワークにマルチキャストメディアサーバーやマルチキャストルーターが設置されており、必要な設定がされている。
・会議資料などをマルチキャストメディアサーバーより無線パソコンへマルチキャスト配信する。

使用機器

対象機器

本製品（WAPM-APG300N/WAPM-AG300N）

必要機器

・マルチキャストメディアサーバー（Windows Server 2003）
・マルチキャストルーター
・クライアントパソコン

設定手順

Webブラウザーを使って、本製品の設定画面へログインし、マルチキャストスヌーピングの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[ネットワーク設定]-[マルチキャスト]をクリックします。

4 以下のように項目を設定して、[設定]をクリックします。

Snooping機能　：使用する（チェックあり）
Snooping対象プロトコル　：お使いの環境に合わせて設定
マルチキャスト無線LAN転送モード　：トンネル転送モードを有効にしない（チェックなし）
フィルタールール　：未学習のマルチキャストパケットを破棄しない（チェックなし）
マルチキャストAging Time　：300（秒）
Router Port　：有線ポート

マルチキャスト設定　? ヘルプ

Snooping 機能	☑使用する
Snooping 対象プロトコル	☑IPv4(IGMP) ☐IPv6(MLD)
マルチキャスト無線LAN 転送モード	☐トンネル転送モードを有効にする
フィルタールール	☐未学習のマルチキャストパケットを破棄する
マルチキャスト Aging Time	300 秒
Router Port	有線ポート(#1)

設定

5 画面左側の[無線設定]－[(使用する無線規格の)無線基本]をクリックします。以下のように項目を設定して、[設定]をクリックします。

SSID　：　Multicast_11A
無線チャンネル　：　任意
モード　：　任意
Multicast Rate　：　お使いの環境に合わせて設定※

※マルチキャスト配信するコンテンツに応じて設定する必要があります。詳しくは、設定画面のヘルプをご参照ください。

6 [設定]をクリックします。

7 画面左側の[無線設定]−[(使用する無線規格の)無線セキュリティー]をクリックします。

以下のように項目を設定して、[設定]をクリックします。

無線の認証	：	WPA2-PSK
追加認証	：	追加認証を行わない
無線の暗号化	：	AES
WPA-PSK(事前共有キー)	：	1234567890(任意の値)、Key更新間隔:60(分)
ANY接続	：	許可する(チェックあり)
プライバシーセパレーター	：	使用しない

無線セキュリティー設定（11a）　? ヘルプ

無線の認証	○認証を行わない ○IEEE802.1x/EAP ○WPA-PSK ◉WPA2-PSK ○WPA/WPA2 mixedmode - PSK ○WPA-EAP ○WPA2-EAP ○WPA/WPA2 mixedmode - EAP
追加認証	◉追加認証を行わない ○MACアドレスリストによる制限 ○MACアドレスリスト+MAC-RADIUS認証 ○MAC-RADIUS認証 認証パスワード ◉MACアドレスを使う ○次のパスワードを使う ○Microsoft NAPを使用する 制限ネットワークに使用するVLAN: 4093
無線の暗号化	○暗号化なし ○WEP(固定値Key) WEP暗号化キー 文字入力・13文字(WEP128) 1: 2: 3: 4: ○WEP(自動配信Key) 自動更新Key長 WEP128 WEP（固定値Key）の併用 併用しない 暗号化キー ○TKIP ◉AES ○TKIP/AES mixedmode WPA-PSK(事前共有キー): •••••••••••••• Key更新間隔: 60 分

［拡張設定］

ANY接続	☑ 許可する
プライバシーセパレーター	使用しない

設定

8 [設定]をクリックします。

以上で本製品の設定は完了です。

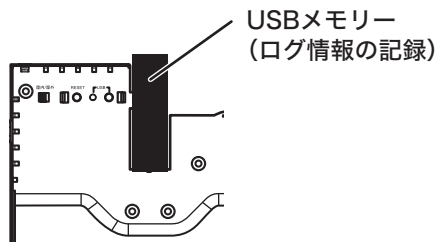
CL設定手順

本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ bridge multicast snooping enable proto all
rtport eth0 aging 300 defaultrule forward
(profile1)man[edit]$ bridge multicast tunnel disable
(profile1)man[edit]$ airset 11a ssid rename ssidnum 1 Multicast_11A
(profile1)man[edit]$ airset 11a channel auto_w52 bandwith 40m
(profile1)man[edit]$ airset 11a mrate 24
(profile1)man[edit]$ airset 11a ssid security ssidnum 1 autu wpa2psk
cipher aes rekey 60 key 1234567890
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

例12:USBメモリーに本製品のログを記録する

本製品に搭載されているUSBポートに別売のUSBメモリーを取り付けると、本製品のログ情報を記録することができます。
ここでは、USBメモリーに本製品のログ情報を記録するために必要な設定を説明します。

構成例

条件

・別売のUSBメモリーを使用する。
・ログ情報をUSBメモリーに記録する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

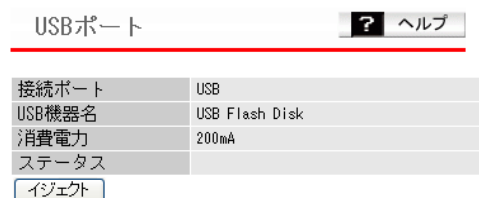
・弊社製USBメモリー
(対応USBメモリーについては、弊社ホームページをご参照ください)

設定手順

Webブラウザーを使って、本製品の設定画面へログインし、Syslog設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[機器診断]－[USB]をクリックします。
「USB機器名」にUSBメモリーの名称が表示されていることを確認します。

4 画面左側の[管理設定]－[ログ情報転送(syslog)]をクリックします。
USBメモリー転送機能の「使用する」にチェックマークをつけて、[設定]をクリックします。

以上で本製品の設定は完了です。

CLI 設定手順

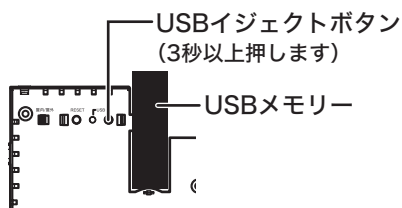
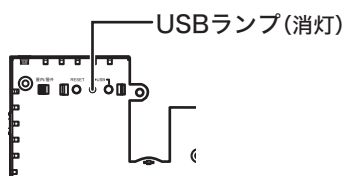
ここまでの設定をCLI を使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ usb show status
(profile1)man[edit]$ setup syslog client usb enable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

ログ情報の確認方法

USBメモリーに転送されたログ情報の確認は、以下の手順でおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、セキュリティーケースから本製品を取り外します。

2 本製品正面のUSBイジェクトボタンを3秒以上押します。

3 USBランプが消灯したら、USBメモリーを抜き取ります。

4 USBメモリーをパソコンに挿して、記録されたログ情報を確認します。

syslog.txt - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

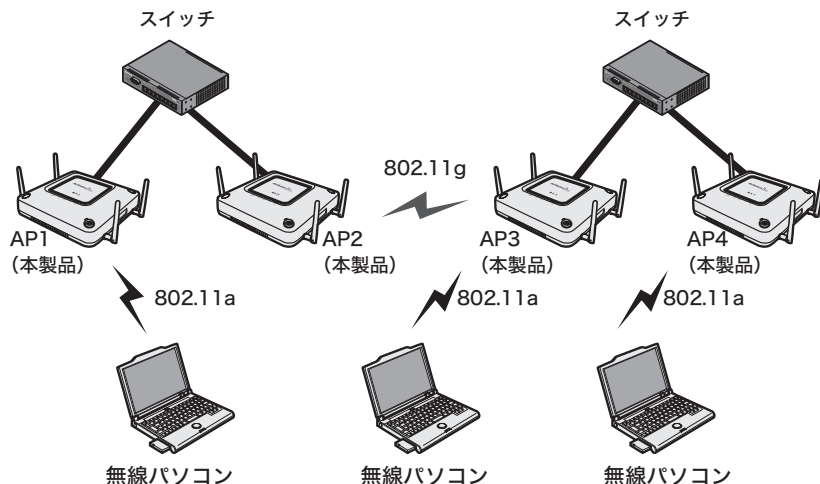
```
Oct 21 10:06:52 2008 [ AP001650107447] : WIRED_ETH: et0: link down
Oct 21 10:06:57 2008 [ AP001650107447] : WIRED_ETH: et0: link up(1000 Mbps Full duplex)
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Request: broadcasting DHCP_DISCOVER
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: broadcasting second DHCP_DISCOVER
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: DHCP_OFFER received from  (192.168.11.1)
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: broadcasting DHCP_REQUEST for 192.168.11.12
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: DHCP_ACK received from  (192.168.11.1)
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : IP Address = 192.168.11.12
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : Subnet Mask = 255.255.255.0
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : Default Gateway = 192.168.11.1
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : DNS[1] = 192.168.11.1
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : DHCPSID = 192.168.11.1
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : DHCPGIADDR = 0.0.0.0
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : DHCPSIADDR = 0.0.0.0
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : DHCPCHADDR = XX:XX:XX:XX:XX:XX
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : DHCPSHADDR = XX:XX:XX:XX:XX:XX
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : DHCPSNAME =
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: Info : LEASETIME(172800) , RENEWALTIME(86400) ,
REBINDTIME(151200)
Oct 21 10:07:04 2008 [ AP001650107447] dhcpcd: add resolve
```

以上でログ情報の確認は完了です。

例13:リピーター機能でローミング環境を構築したい

本製品のリピーター(WDS)機能を使用して、ローミング環境を構築する方法を説明します。

⚠注意 本設定事例では、802.11aと802.11gの同時通信が必要となりますので、WAPM-AG300Nをお使いの方は、本設定事例通りの設定はできません。

構成例

条件

・WAPM-APG300Nを使用している。
・AP1－AP2間、およびAP3－AP4間は、有線接続する。
・AP2－AP3間は、802.11gを使用してリピーター(WDS)通信する。
・各AP－無線パソコン間は、802.11aを使用して通信する。
・無線パソコンがローミングできるように、本製品の設定はすべて共通化する。

使用機器

対象機器

本製品(WAPM-APG300N)

必要機器

・クライアントパソコン
・有線側ネットワーク機器(例:スイッチなど)

設定手順(AP1～4共通の設定)

Webブラウザーを使って、本製品の設定画面へログインし、802.11aの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[無線設定]－[(802.11aの)無線基本]をクリックします。
以下のように項目を設定して、[設定]をクリックします。

SSID ： kaihatsu
無線チャンネル ： Auto(W52)(任意のチャンネル)
モード ： 倍速モード

4 [設定]をクリックします。

5 画面左側の[無線設定]－[(802.11aの)無線セキュリティー]をクリックします。以下のように項目を設定して、[設定]をクリックします。

無線の認証	：	WPA2-PSK
追加認証	：	追加認証を行わない
無線の暗号化	：	AES
WPA-PSK	：	1234567890(任意の値)、Key更新間隔：60(分)
ANY接続	：	許可する
プライバシーセパレーター	：	使用しない

6 [設定]をクリックします。

以上でAP1～4共通の設定は完了です。
続けて、AP2とAP3にリピーター機能の設定をします。

設定手順(AP2、3のリピーター機能の設定)

Webブラウザーを使って、本製品の設定画面へログインし、リピーター機能の設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

3 画面左側の[無線設定]−[(802.11gの)無線基本]をクリックします。
以下のように項目を設定して、[設定]をクリックします。

無線チャンネル ： 1 チャンネル(Auto以外の任意のチャンネル)
モード ： 倍速モード

4 [設定]をクリックします。

5 画面左側の[無線設定]－[(802.11gの)リピーター機能]をクリックします。
「リピーター機能(WDS)」を「WDS専用モードで使用する」に変更して、[設定]をクリックします。

6 [設定]をクリックします。

7 [通信可能なアクセスポイントの編集]をクリックします。

8 画面左側の[無線設定]−[(802.11gの)リピーター機能]をクリックします。以下のように項目を設定して、[新規追加]をクリックします。

アクセスポイントの無線側MACアドレス:アクセスポイントの無線側MACアドレス
VLANモード : Untagged Port
無線の暗号化 : AES
WEP/PSK : 9876543210(任意の値)

リピーター機能(WDS)設定 − 通信可能なアクセスポイントの編集 (11g) ? ヘルプ

編集を終了して前の画面へ戻る

通信可能なアクセスポイントの新規追加 ? ヘルプ

アクセスポイントの無線側MACアドレス	XX:XX:XX:XX:XX:XX
VLAN モード	Untagged Port VLAN ID 1
暗号化	AES
WEP/PSK	●●●●●●●●●●

本機の無線側MACアドレス[XX:XX:XX:XX:XX:XX]

新規追加

通信可能なアクセスポイント ? ヘルプ

MACアドレス	暗号化	VLAN ID	状態	操作
通信可能なアクセスポイントが登録されていません				

9 もう1台のエアステーションにも同様の設定をおこないます。

以上で設定は完了です。

CLI設定手順(AP1〜4共通の設定)

AP1〜4の共通設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11a ssid rename ssidnum 1 kaihatsu
(profile1)man[edit]$ airset 11a channel auto_w52 bandwidth 40m
(profile1)man[edit]$ airset 11a ssid security ssidnum 1 auth wpa2psk
cipher aes rekey 60 key 1234567890
(profile1)man[edit]$ airset 11a ssid anyscan ssidnum 1 enable
(profile1)man[edit]$ airset 11a ssid ssidnum 1 privacy disable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

CLI設定手順(AP2、3のリピーター機能の設定)

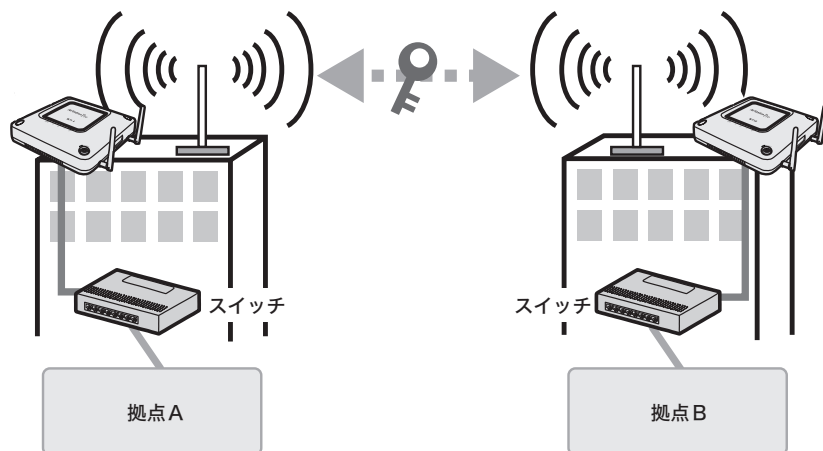
AP2、3のリピーター機能の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11g channel 1 40m subch 5
(profile1)man[edit]$ airset 11g wds exclusive
(profile1)man[edit]$ airset 11g wds add XX:XX:XX:XX:XX:XX
(profile1)man[edit]$ airset 11g wds vlan 1 mode untagged vlanid 1
(profile1)man[edit]$ airset 11g wds security XX:XX:XX:XX:XX:XX
wpapsk cipher aes key 9876543210
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

例14：リピーター機能で拠点間を無線接続したい

本製品のリピーター（WDS）機能を使用して、拠点間を無線接続する方法を説明します。

⚠注意 本設定事例では、802.11aと802.11gの同時通信が必要となりますので、WAPM-AG300Nをお使いの方は、本設定事例通りの設定はできません。

構成例

条件

・802.11a（W56帯）または802.11gを使用して、拠点間を無線接続する。
・暗号化はAESを使用する。
・本製品の屋内/屋外スイッチを「屋外」に切り替える。

使用機器

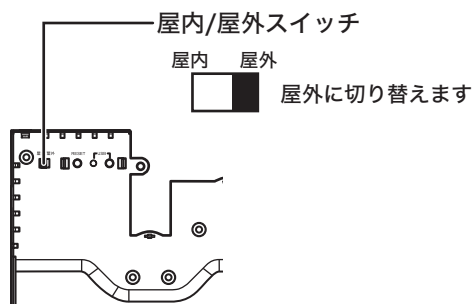
対象機器

本製品（WAPM-APG300N/WAPM-AG300N）

必要機器

・屋外設置アンテナ（WLE-HG-NDC/A（別売）やWLE-HG-DA/AG（別売）など）
・屋外アンテナ用同軸ケーブル（WLE-CCシリーズ（別売））
・同軸ケーブル変換コネクター（WLE-OP-RNC（別売））

設定手順

1 本製品前面の屋内/屋外スイッチを「屋外」に切り替えます。

⚠注意 ・スイッチを「屋外」に設定すると、802.11a通信時にW56チャンネル(100/104/108/112/116/120/124/128/132/136/140ch)のみ使用可能となります。
・W52(36/40/44/48ch)およびW53(52/56/60/64ch)チャンネルを屋外で使用すると、電波法違反となりますので、ご注意ください。

2 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

3 「詳細設定」をクリックします。

4 画面左側の[無線設定]－[(使用する無線規格の)無線基本]をクリックします。以下のように項目を設定して、[設定]をクリックします。

無線チャンネル：100チャンネル(AutoおよびW52/W53以外の任意のチャンネル)
モード　　　　：倍速モード

無線基本設定 (11a)　？ ヘルプ

無線機能	☑使用する
SSID	◉ エアステーションのMACアドレスを設定(XXXXXXXXXXXX_A) ○ 値を入力：
VLAN ID	1
無線チャンネル	100 チャンネル(DFSあり) ※DFSありの場合、気象レーダー等を感知すると自動的にチャンネルが変更されます モード　倍速モード(40MHz, +104ch)

[拡張設定]

無線モード	11aと11nを同時利用する

⚠注意
- 802.11aを使って拠点間を無線接続する場合は、必ずW56チャンネル(100/104/108/112/116/120/124/128/132/136/140ch)をご使用ください。W52(36/40/44/48ch)およびW53(52/56/60/64ch)チャンネルを使用すると、電波法違反となります。
- W56チャンネル使用時に本製品が中継機が気象レーダー等の発する電波検出すると、同じ周波数帯を使わないよう無線チャンネルが自動的に変更されます。(DFS(Dynamic Frequency Selection)機能)
無線チャンネル変更時は1分ほど通信ができなくなりますので、ご注意ください。

5 画面左側の[無線設定]－[(使用する無線規格の)リピーター機能]をクリックします。「リピーター機能(WDS)」を「WDS専用モードで使用する」に変更して、[設定]をクリックします。

リピーター機能(WDS)設定 (11a)　？ ヘルプ

リピーター機能(WDS)	使用しない 使用しない 使用する WDS専用モードで使用する

[設定]

※リピーター機能を使用するには通信する無線機と
IPアドレスが重複しないようにして下さい。

通信可能なアクセスポイント　？ ヘルプ

MACアドレス	暗号化	VLAN ID	状態
通信可能なアクセスポイントが登録されていません			

[通信可能なアクセスポイントの編集]

(本機の無線側MACアドレス[XX:XX:XX:XX:XX:XX])

6 [設定]をクリックします。

7 [通信可能なアクセスポイントの編集]をクリックします。

8 画面左側の[無線設定]－[(使用する無線規格の)リピーター機能]をクリックします。
以下のように項目を設定して、[新規追加]をクリックします。

アクセスポイントの無線側MACアドレス:アクセスポイントの無線側MACアドレス
VLANモード　：　Untagged Port
無線の暗号化　：　AES
WEP/PSK　　：　9876543210(任意の値)

リピーター機能(WDS)設定 － 通信可能なアクセスポイントの編集 (11a) ? ヘルプ

編集を終了して前の画面へ戻る

通信可能なアクセスポイントの新規追加 ? ヘルプ

アクセスポイントの無線側MACアドレス	XX:XX:XX:XX:XX:XX
VLAN モード	Untagged Port　VLAN ID 1
暗号化	AES
WEP/PSK	●●●●●●●●●●●

本機の無線側MACアドレス[XX:XX:XX:XX:XX:XX]

新規追加

通信可能なアクセスポイント ? ヘルプ

MACアドレス	暗号化	VLAN ID	状態	操作
通信可能なアクセスポイントが登録されていません				

9 もう1台のエアステーションにも同様の設定をおこないます。

10 屋外アンテナのマニュアルを参照して、屋外アンテナを設置します。

11 別冊の「ユーザーズマニュアル」を参照して、本製品と屋外アンテナを同軸ケーブルで接続します。

以上で設定は完了です。

CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$


802.11aを使用する場合

(profile1)man[edit]$ airset 11a channel 100 40m subch 104
(profile1)man[edit]$ airset 11a wds exclusive
(profile1)man[edit]$ airset 11a wds add XX:XX:XX:XX:XX:XX
(profile1)man[edit]$ airset 11a wds vlan 1 mode untagged vlanid 1
(profile1)man[edit]$ airset 11a wds security XX:XX:XX:XX:XX:XX
wpapsk cipher aes key 9876543210


802.11gを使用する場合

(profile1)man[edit]$ airset 11g channel 1 40m subch 5
(profile1)man[edit]$ airset 11g wds exclusive
(profile1)man[edit]$ airset 11g wds add XX:XX:XX:XX:XX:XX
(profile1)man[edit]$ airset 11g wds vlan 1 mode untagged vlanid 1
(profile1)man[edit]$ airset 11g wds security XX:XX:XX:XX:XX:XX
wpapsk cipher aes key 9876543210


(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```